POLICY BRIEFS SERIES

Deploying the Once-Only Policy Supplement

The OOP Readiness Framework

Naeha Rashid
David Eaves, ***Series Editor***

NOVEMBER 2020

HARVARD Kennedy School
ASH CENTER
for Democratic Governance
and Innovation

POLICY BRIEFS SERIES

Deploying the Once-Only Policy Supplement

The OOP Readiness Framework

Naeha Rashid
David Eaves, *Series Editor*

NOVEMBER 2020

A PUBLICATION OF THE

Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

617-495-0557
ash.harvard.edu

About the Ash Center

The Roy and Lila Ash Center for Democratic Governance and Innovation advances excellence and innovation in governance and public policy through research, education, and public discussion. By training the very best leaders, developing powerful new ideas, and disseminating innovative solutions and institutional reforms, the Center's goal is to meet the profound challenges facing the world's citizens. The Ford Foundation is a founding donor of the Center. Additional information about the Ash Center is available at ash.harvard.edu.

This research paper is one in a series published by the Ash Center for Democratic Governance and Innovation at Harvard University's John F. Kennedy School of Government. The views expressed in the Ash Center Policy Briefs Series are those of the author(s) and do not necessarily reflect those of the John F. Kennedy School of Government or of Harvard University. The papers in this series are intended to elicit feedback and to encourage debate on important public policy challenges.

About the Author

Naeha Rashid has worked at the intersection of financial inclusion, social entrepreneurship, and technology for the last several years. She is passionate about leveraging technology solutions to improve the quality and character of people's lives. While a 2019–20 digital governance fellow at Harvard Kennedy School's Ash Center, Rashid analyzed issues related to technology and innovation in government. Previously, Rashid worked for CGAP—a member of the World Bank Group—leading her team's work in Pakistan to catalyze innovation and scaling of digital financial services. She was also a core member of the start-up team for Karandaaz Pakistan, an organization funded by the Bill and Melinda Gates Foundation. Rashid holds a Master in Public Policy from Harvard Kennedy School and undergraduate dual degrees in International Development (honors) and Economics from McGill University. Find her online.

About the Series Editor

David Eaves is a lecturer of Public Policy at the Harvard Kennedy School where he teaches on digital transformation in Government. In 2009, as an adviser to the Office of the Mayor of Vancouver, David proposed and helped draft the Open Motion which created one of the first open data portals in Canada and the world. He subsequently advised the Canadian government on its open data strategy where his parliamentary committee testimony laid out the core policy structure that has guided multiple governments approach to the issue. He has gone on to work with numerous local, state, and national governments advising on technology and policy issues, including sitting on Ontario's Open Government Engagement Team in 2014–2015.

In addition to working with government officials, Eaves served as the first Director of Education for Code for America—training each cohort of fellows for their work with cities. Eaves has also worked with 18F and the Presidential Innovation Fellows at the White House providing training and support.

Acknowledgments

Financial support for this paper was provided by the Council of Arab Economic Unity (CAEU) of the League of Arab States. The CAEU was not involved in the research required to prepare this report and had no role in shaping the findings presented.

This supplementary paper required a significant amount of additional work. Thank you to David Eaves for his unwavering and patient support; this paper would not have materialized without his guidance. Thank you to Angelo Mikael, who acted as my sole research assistant and spent many hours brainstorming, researching, and identifying thought partners who would be able to help us.

Finally, this work would not have been possible without the invaluable insights of our interview partners: Lebanese University professor Nadim Mansouri; Fadi Khoury, CEO of LevantNET; Gilbert Doumit, managing partner of Beyond Reform and Development; Issa Mahasneh, executive director of Jordan Open Source; Tareq Saraireh, business development manager of AI at Mawdoo3.com; Mothanna Gharaibeh, minister of Digital Economy and Entrepreneurship, Jordan; and Chetan Choudhury, an advisor in the office of the prime minister of the United Arab Emirates.

Contents

Part 1: Introducing the Readiness Framework

Under the once-only policy, users have to provide diverse data only once when in contact with public administrators. After the initial data transfer, various government departments can internally share and reuse the data to create public value and better service users. OOP has exciting positive transformative potential as a tool that can create public value, reduce the cost of government, and spur governments toward next-generation digitization.

In "Deploying the Once Only Policy: A Privacy-Enhancing Guide for Policymakers and Civil Society Actors," I shared my understanding of OOP, examined the potential benefits of this policy, and shared the core enablers I believe must be put in place to ensure a successful OOP deployment. These core enablers are a privacy framework, an identification mechanism, and a data-sharing mechanism.

While the guide shares how countries can institute OOP from scratch in a privacy-enhancing way, it does not explicitly answer an equally fundamental question: **Under current conditions is your country ready for OOP implementation?** To address this outstanding issue, I have leveraged my prior work to create an OOP readiness framework that will allow countries to assess where they stand across each OOP enabler.

The readiness framework aims to answer three questions:

- Are the underlying enablers needed for OOP in place?
- What shortfalls exist in the design and implementation of these underlying pieces?
- What is an optimal OOP strategy under current conditions?

The framework acknowledges that many countries will not be starting from scratch in the OOP stack-development process and may need to optimize elements of existing systems instead. A summary of my simple framework can be seen in Table 1 below.

Table 1: The OOP readiness framework[1]

CORE OOP ENABLER	ELEMENTS OF ENABLER	KEY QUESTIONS
Privacy framework	• Data-privacy and data-protection regulations • Privacy-by-design principles • Enforcement	• Is the key enabler in place? • Is the key enabler applicable and/or leverageable across government departments and all tiers of government? • Is the key enabler sufficiently strong? • Have sufficient protections around the key enabler been put in place to prevent current or future misuse?
Identification mechanism	• Unique identifier	
Data-sharing mechanism	• Data classification • Data exchange	

[1] For more information about the core OOP enablers and how they can be optimally designed, please refer to the policymakers' guide.

In this supplement to the policymakers' guide, I will deploy the readiness framework using the example of three digital Arab League (DAL) countries: Lebanon, Jordan, and the United Arab Emirates (UAE). Based primarily on online research, my findings have been bolstered by semi-structured interviews with digital-government experts across these three nations.

In addition to these three comprehensive assessments, my research assistant and I have conducted shorter assessments of ten other DAL countries based wholly on online research and meant to indicate areas where further work would likely be needed if OOP were to be deployed. Notably, all the countries in this work have been chosen with a view toward optimizing geographical distribution while avoiding the assessment of those Arab League nations currently impacted by violent conflicts.

Part 2: Implementing the OOP Readiness Framework

2.1 Lebanon

Table 2: State of digital penetration in Lebanon

	Digital Penetration in Lebanon *Population: 6.84 million*	
	Number of users	Percentage of users as a proportion of population
Internet	5.35 million	78%
Mobile phone	4.65 million	68%
Social media	4.10 million	60%

Data Source: Various World Bank and UN reports as compiled by datareportal.com

Despite achieving a fair level of digital penetration (see Table 2 above), government digitization in Lebanon is still nascent. Though several digitization strategies have been launched—some as far back as the early 2000s—strategy implementation has been a major problem. The broad consensus among experts is that Lebanon has not risen to its potential in the digital government space; as a result, public entities remain entrenched in bureaucracy and paperwork. Major barriers to past efforts included:[2]

- Lack of political will, capacity, and institutions that can lead the reform work needed in the digitization space
- The absence of a unifying vision to help public entities harmonize actions and identify needed core connected government infrastructure[3]
- Poor perception of public institutions and public servants

However, recent developments in the government digitization space show signs for optimism.

- Digital economy reform has been **highlighted as a key priority area at the highest levels of government,**[4] including by the prime minister and the president. Government digitization in particular has been emphasized as a way of restoring trust between the state and its citizens.

[2] Paul Welton, Peter McConaghy, and Samia Melhem, "Lebanon:Digital Economy Project," World Bank, October 30, 2018, http://documents1.worldbank.org/curated/en/933171540902301709/pdf/Concept-Project-Information-Document-Integrated-Safeguards-Data-Sheet-LB-Digital-Economy-Project-P167643.pdf.
[3] Thomas Schellen, "Lebanon is finally seeking to leapfrog into digitally empowered spheres," *Executive Magazine*, October 7, 2019, https://www.executive-magazine.com/economics-policy/lebanon-is-finally-seeking-to-leapfrog-into-digitally-empowered-spheres.
[4] "Lebanon Digital Transformation Strategy 2018," Lebanon Digital Transformation and the Republic of Lebanon, Office of the Minister of State for Administrative Reform, https://www.omsar.gov.lb/getattachment/b4b8b496-d357-49dc-bd85-a6a850c088e4/Digital-Transformation-Strategy-in-Lebanon.

- A **comprehensive government digitization strategy** was released in 2018.[5] Known as the Digital Transformation Strategy, the initiative is being spearheaded by the Office of the Minister of the State for Administrative Reform, and it clearly lays out key goals and pillars, highlighting many concepts that are in line with OOP, including the creation of common digital and data platforms, the need for strong cybersecurity and privacy, and the promotion of collaborative local schemes funded by government and donors.
- **The World Bank is contributing US$200 million to funding key aspects of the plan**, including governance, service efficiency, public-private partnerships, and institutionalizing government digitization.[6] The project proposal passed its initial review stage in 2018 and is likely to go live in the coming year.

2.1.1 OOP Readiness Analysis

To understand Lebanon's current state of OOP readiness, we will examine where it currently stands across each of the OOP enablers.

2.1.1.1 Privacy Framework

a. Regulations

Current status: Internationally, Lebanon is a signatory to at least eleven treaties with privacy implications, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Arab Charter on Human Rights.[7] The Lebanese constitution doesn't explicitly mention or guarantee a right to privacy, but some experts believe that Articles 8 and 13—which indirectly protect individual liberty and freedom of expression—can be interpreted as privacy protections.

Lebanon's main data-related regulation is the Electronic Transactions and Personal Data Law that came into effect in 2018. Introduced in 2004, the law is primarily concerned with e-commerce and e-signatures. It addresses any collection, processing, or use of personal data, whether via electronic means or otherwise, and determines the conditions that must be satisfied in order for data collection (data minimization and limitation), processing, and retention, and the use of personal data, to be legal.

Gaps: While the passing of the E-Transactions Law has been seen as an important step in creating a digital Lebanon, it is considered outdated in comparison to more modern frameworks such as the European Union's General Data Protection Regulation (GDPR) and has several weaknesses:

- It neglects to define and guarantee a right to data privacy and fails to create general principles around data access and use for Lebanese citizens and residents.
- Its legal framework does not sufficiently address data protection. For example, the law fails to offer sufficient legal protection for people's rights to data agency, to redressal, to rectification of collected personal data, and to protection against unethical uses of their personal data.
- The consent requirement is not clearly defined in the law and seems *a posteriori* (after the fact). While technically the law requires informed consent from the data subject, this is not enforced if the data-

[5] "Lebanon Digital Transformation Strategy 2018."
[6] LB Digital Economy Project, World Bank, https://projects.worldbank.org/en/projects-operations/project-detail/P167643?lang=en&tab=documents&subTab=projectDocuments.
[7] "State of Privacy Lebanon," Privacy International, January 27, 2019, http://privacyinternational.org/state-privacy/1081/state-privacy-lebanon.

collecting entity can prove that the circumstances made it difficult to obtain such consent (Article 88).[8] Though data subjects can oppose the collection of their personal data, they can't do so if they previously provided consent to the data collector (Article 94).[9] The type of consent—implicit or explicit—is unspecified, and there are many similar gaps that can be exploited by data processing bodies.

- The scope of the law is not clearly specified, the default assumption being that it applies to all residents and not only to citizens, as long as it involves actors (data collector/processor and data subject) in Lebanon.

b. Privacy-by-design principles

Current status and gaps: To my knowledge there is no explicit or implicit mention of using privacy-by-design principles across Lebanon's existing privacy framework.

c. Enforcement

Current status: According to the E-Transactions Law, the processing and oversight of personal data, including handling data-processing requests, is concentrated in the executive branch of the government under the Ministry of Economy and Trade.

Technically, entities that want to collect, process, and use personal data must either provide a declaration or obtain a license from the Ministry of Economy. Additionally, both the Ministry of Interior and Municipalities and the Ministry of Defense have been granted limited but dangerous oversight over the processing of personal data. Article 97 gives them the power to award licenses for any data pertaining to "external and internal security of the state" but does not define this term.[10]

While the consequences of a data breach are unclear, the E-Transactions Law does specify criminal provisions related to cyber-hacking.

Gaps: Lebanon does not have a separate data-protection authority.[11] Oversight is concentrated under the Ministry of Economy, which is an unorthodox structure when compared with global examples. Other countries, such as those in the European Union, have created independent data-protection authorities with representation from across various branches and ministries of government to ensure the system contains adequate checks and balances.[12] Notably, while some of the Ministry of Economy's data-oversight powers may end up devolving to the new, as-yet-unnamed, Lebanese national cybersecurity body, this is yet to be institutionalized.[13]

Despite the requirement for declaration to and licensing by the Ministry of Economy, the Lebanese law includes a long list of exceptions that allow data-processing entities to operate without providing a declaration or obtaining a license. Similarly, the limits around licensing by the ministries of the Interior and Defense are unspecified and unclear.

Finally, other than the criminalization of cyber-hacking, no real accountability mechanisms have been created or defined under the law. Though the 2017 Right to Access to Information Law would theoretically require data-

[8] Sanaa Eter, "The Lebanese E-transaction Law In Relation with Personal Data Protection," blog, April 30, 2019, https://medium.com/data-and-society/the-lebanese-e-transaction-law-in-relation-with-personal-data-protection-26e6112322f1.
[9] "An 'Ugly' New Data Protection Law in Lebanon," *SMEX* blog, October 11, 2018, https://smex.org/an-ugly-new-data-protection-law-in-lebanon/.
[10] "An 'Ugly' New Data Protection Law in Lebanon."
[11] "State of Privacy Lebanon."
[12] "An 'Ugly' New Data Protection Law in Lebanon."
[13] "Lebanon is finally seeking to leapfrog into digitally empowered spheres."

processing companies to notify Lebanese data subjects of any data breaches, there is an exception in the law around sensitive and classified documents as specified by the ministries of Interior and Defense.

Table 3: Summary assessment of privacy framework in Lebanon

Privacy framework in Lebanon			
Element	**Manifestation**	**Summary**	**Gaps**
Regulations	Electronic Transactions and Personal Data Law 2018	• Is primarily concerned with e-commerce and e-signatures • Addresses only some aspects of data collection, processing, and use	• Does not address data privacy or data protection • Access rights are not adequately specified • Consent requirements are not clearly stated • Scope of the law is not clearly defined
Privacy-by-design principles	Do not appear to be part of the framework		
Enforcement	Ministry of Economy and Trade Ministry of Interior Ministry of Defense	• Licensing for data collection from the Ministry of Economy is required unless the entity falls under an exempted group • Licensing power also rests with the ministries of Interior and Defense • Cyber-hacking is a prosecutable offense	• No independent data-protection authority exists • The licensing process lacks clarity and transparency • No real accountability mechanisms beyond criminalization of cyber-hacking

2.1.1.2 Identification Mechanism: Unique Identifier

Current status: All Lebanese citizens aged 15 or older and residing in the country are legally obligated to apply for the Lebanese identity card,[14] which provides unique biometric identification (thumbprint) and is connected to a unique 12-digit alphanumeric identifier in the national identity database (NID).[15] The card and the NID fall under the purview of the Ministry of Interior and Municipalities.[16] Noncitizen residents can apply for biometric-based residence permits, which are also issued by the Ministry of the Interior.[17]

The unique identifier on identity and resident cards are currently leveraged by several other services, such as health,

[14] https://www.dawlati.gov.lb/.
[15] United Nations High Commissioner for Refugees, "Lebanon: Information on National ID Cards," Refworld, July 22, 2016, https://www.refworld.org/docid/5843f4b74.html.
[16] https://www.dawlati.gov.lb/.
[17] "State of Privacy Lebanon."

banking, and job search.[18]

Gaps: Because there is no clear legal framework regulating the use of biometrics as a basis for unique identification in Lebanon, the data collected is at risk of being used for surveillance.

Anecdotally it appears that under the current status quo the unique number is also highly exposed, because methods such as tokenization have not been implemented.

Table 4: Summary assessment of identification mechanism in Lebanon

Identification mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Unique identifier	Lebanese identity cards and resident permits	Unique biometric identifier issued to citizens via the Lebanese identity card, and to residents via resident permits.	• No legal basis for biometric data collection. • Unique identifier appears to be highly exposed.

2.1.1.3 Data-Sharing Mechanism

Current status and gaps: All elements of standardized data sharing (classification and data exchange) appear to be at a nascent stage in Lebanon at this time. No common data-classification standards are applied across all of government. Interdepartmental data exchange appears to occur on an ad hoc basis between individual departments and ministries with no common technology or institutional governance in place.

Table 5: Summary assessment of data-sharing mechanism in Lebanon

Data-sharing mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Data classification	No standardized data classification system is used at this time		
Data exchange	Ad-hoc data exchange		

2.1.2 OOP Assessment

Lebanon is currently just beginning government digitization and is not ready for a principle approach to OOP implementation. Several things must be built before the country arrives at the necessary level of institutional maturity, including:

- Strengthened legal frameworks in the areas of privacy, data protection, and unique identifiers

[18] https://www.dawlati.gov.lb/.

- Necessary all-of-government technology infrastructure and governance arrangements, particularly in the area of a common data-sharing mechanism
- Transformation of internal government culture so that it is more digitally oriented and better prepared for cross-departmental collaboration
- Increased trust between the government and citizen, which, based on anecdotal evidence, at this stage appears to be relatively low

Once the legal frameworks have been sufficiently strengthened, the Lebanese government may consider embarking on its OOP journey by experimenting with an inherently limited program such as death notification. For more information on how this can be designed please refer to the UK experience as detailed in the "Deploying the Once-Only Policy."

2.2 Jordan

Table 6: State of digital penetration in Jordan

	Digital penetration in Jordan *Population: 10.15 million*	
	Number of users	Percentage of users
Internet	9.01 million	89%
Mobile	8.63 million	85%
Social media	5.70 million	56%

Data source: Various World Bank and UN reports as compiled by datareportal.com

According to the World Bank's most recent data, Jordan's digital economy grew nearly 12 percent between 2014 and 2018. Information and communications technology (ICT) activities added revenues of US$300 million to the economy during that period,[19] and mobile and internet penetration rates reached 85 percent and 88.8 percent, respectively (see Table 6). Though the numbers have not yet been released, Jordan's biggest strides in digital development have taken place in the last two years, so future data will likely show even greater improvements.

Beyond advancing the overall digital economy, the Jordanian government has had a long-standing commitment to digitization. Though Jordan has consistently outperformed the world average on the UN's E-Government Development Index, the general perception is that Jordan still has a long road ahead in this area. Experts have flagged the following areas of concern:[20]

- Lack of cohesion and coordination across government departments
- General resistance to change among government workers
- Limited government spending

[19] "Jordan: US$200 million to improve digital services and access to jobs for youth and underserved communities," World Bank, March 20, 2020, https://www.worldbank.org/en/news/press-release/2020/03/20/jordan-us200-million-to-improve-digital-services-and-access-to-jobs-for-youth-and-underserved-communities.
[20] "E-Government in Jordan: A Guide for Policymakers," Jordan Strategy Forum, July 2019, http://jsf.org/sites/default/files/EN%20E-Government%20Report%20.pdf.

- Trouble retaining qualified staff in government

Despite these issues, significant strides have been made in recent years, including:

- The **launch of e-government services** across various departments in 2018.[21] The Jordanian government has streamlined resident and citizen access to these e-services via a single consolidated portal, jordan.gov.jo, whose purpose is to provide seamless integrated service delivery to citizens and businesses and to digitize payments associated with government services. So far approximately 340 of 500 total services have been digitized.
- The introduction of **the Ministry for Digital Economy and Entrepreneurship** (MoDEE) in May 2019.[22] MoDEE's mandate is to deliver and manage the government's digital transformation agenda for all Jordanian public entities so as to facilitate the delivery of end-user services to citizens and businesses.
- The approval of a **US$200 million "Youth, Technology and Jobs" project** funded by the World Bank in March 2020.[23] Part of the fund will be used to expand government digital services. The goal of is to digitize 80 percent of government payments and mobilize around US$20 million in new private-sector investments in digital services.

2.2.1 OOP Readiness Analysis

2.2.1.1 Privacy Framework

a. Regulations

Current status: Internationally, Jordan is a signatory to at least six treaties with privacy implications, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Arab Charter on Human Rights.[24]

Articles 7 and 18 of the Jordanian constitution guarantee the inviolability of the private life of Jordanians and the privacy of their communications.[25]

There are currently no legal data privacy or protection laws in Jordan. A draft data-protection bill that was originally submitted for review by the Ministry of Communications (now MoDEE) in 2014 was in its fourth and final draft as of December 2019.[26] The draft personal-data-protection bill, which is applicable to all private and public institutions in Jordan, is partially aligned with core aspects of the EU's GDPR, mirroring the GDPR's concepts of transparency, accuracy, storage limitation, and data minimization.

Gaps: Though the draft data-protection bill has changed significantly and is yet to be enforced, even in its current form the bill raises major concerns, as it fails to incorporate international standards and best practices and provides insufficient consideration for modern forms of data processing, such as giving a data processor one month to comply

[21] "State of Privacy Jordan," Privacy International, January 26, 2019, http://privacyinternational.org/state-privacy/1004/state-privacy-jordan.
[22] Ali Abukumail, "Digitalizing a pathway to growth in Jordan," blog, World Bank, June 27, 2019, https://blogs.worldbank.org/arabvoices/digitalizing-pathway-growth-jordan.
[23] "Jordan: US$200 million to improve digital services and access to jobs for youth and underserved communities."
[24] "State of Privacy Jordan."
[25] "State of Privacy Jordan."
[26] Raya Sharbain, "Data protection policy void threatens privacy rights of citizens and refugees in Jordan," Global Voices Advocacy (blog), December 30, 2019, https://advox.globalvoices.org/2019/12/30/data-protection-policy-void-threatens-privacy-rights-of-citizens-and-refugees-in-jordan/.

when a data subject withdraws consent for data processing.[27] The draft also insufficiently addresses issues of oversight and enforcement.

b. Privacy-by-design principles

Current status and gaps: To my knowledge there is no explicit or implicit mention of using privacy-by-design principles within Jordan's existing privacy framework.

c. Enforcement

Current status: There is currently no body enforcing data privacy or protection in Jordan.

Gaps: The draft data-protection bill proposes the creation of the Jordan Privacy Commission—but the independence of this body is a major concern to critics of the bill. Under the current draft, the commission will not only be appointed by the executive arm of the government, but will also be chaired by the ICT minister.[28] In addition, members of the security forces will have two seats on the commission; this particular point is a source of deep concern for civil-society actors. Moreover, the suggested structure is not in line with international standards, as it is extremely intertwined with the government and gives the commission insufficient independence.[29]

Table 7: Summary assessment of privacy framework in Jordan

Privacy Framework in Jordan			
Element	**Manifestation**	**Summary**	**Gaps**
Regulations	Data Protection Bill (4th and final draft)	• Aligned with GDPR around the concepts of transparency, accuracy, storage limitation, and data minimization • Applicable to all private and public institutions in Jordan	• Not implemented • Concerns around issues of data processing • Concerns around proposed Jordan Privacy Commission
Privacy-by-design principles	Do not appear to be part of the framework		
Enforcement	Jordan Privacy Commission (proposed)	Government-appointed and -chaired body	• Not established. • Concerns around commission structure and lack of independence

[27] "Data Privacy Frameworks in MENA: Emerging approaches and common principles," GSMA and PwC, November 2019, https://www.gsma.com/mena/wp-content/uploads/2019/12/GSMA-Data-Privacy.pdf.
[28] "Data protection policy void threatens privacy rights of citizens and refugees in Jordan."
[29] "Data Privacy Frameworks in MENA."

2.2.1.2 Identification Mechanism

Unique identifier

Current status: The Jordan personal identification card is issued to all citizens over 18. Each card is linked to a 10-digit unique identifier known as the national number.[30]

Updated in June 2016 and required by early 2018, the new smart ID card includes 18 data fields—such as gender, name (in Arabic and English), place of birth, place of residence, and blood type[31]—some of which is stored in the card's electronic microprocessor and does not appear printed on the card. The card is issued by the Department of Civil Status and Passports, which is housed in the Ministry of the Interior.[32]

One of the reasons for upgrading the card was to create a reliable online infrastructure for access to future e-Government services. There are plans to integrate the ID card with driver's license information, health insurance data, or other databases.[33]

Gaps: No specific regulations have been adopted to regulate the deployment of the smart ID card, and the lack of a data-protection law, as mentioned earlier, leaves this kind of initiative without clear regulation for the processing and security of personal data. In addition, the national number is highly exposed and is even published publicly with the electoral register.

Table 8: Summary assessment of identification mechanism in Jordan

Identification mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Unique identifier	Jordan Personal Card	• Unique identifier linked to the smart card	• No legal basis for securing data • National number is highly exposed

2.2.1.3 Data-Sharing Mechanism

a. Data classification

Current status: Jordan joined the Open Government Partnership in 2011 and launched an open data policy in 2017. By implementing the open data policy, the Jordanian government seeks to facilitate access to data in the government's possession and evaluate the quality of the data provided.[34]

While a few government departments have created private data registers that they make available to other departments—the most significant of them being the Civil Registry—there is no process-standardization to date.

---

[30] "State of Privacy Jordan."
[31] "Jordan launches its new national ID card program," Thales, accessed October 6, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/national-id-card-jordan.
[32] "Identification for Development (ID4D) Global Dataset," Data Catalog, World Bank, accessed January 13, 2020, https://datacatalog.worldbank.org/dataset/identification-development-global-dataset.
[33] "Jordan launches its new national ID card program."
[34] "Jordan: Implement an Open Data Sources Policy," Open Government Partnership, accessed August 10, 2020, https://www.opengovpartnership.org/members/jordan/commitments/JO0056/.

The Jordanian government is in the midst of building a data-structure "bible" that will provide guidance to government entities on a common system format to facilitate the transfer of data.

Gaps: Common data-structure standards that are applied across all of government are at a very initial stage of development at this time. It is unclear how these will be rolled out in the future.

No common data-sensitivity framework exists at this time.

b. Data exchange

Current status: The Government Service Bus (GSB) is the primary technology layer departments can use to move data around the government. Middleware, the GSB "unifies and connects applicable services, applications and resources within the government of Jordan" with the aim of facilitating exchange of shared data across government agencies.[35]

Gaps: While the technology layer is technically present, it is unclear how many departments are currently using it and/or how many use cases it is facilitating. Conversations with civil society actors suggest that use of the GSB is low and that interdepartmental data exchange is still occurring on a largely bilateral basis between individual departments and ministries.

Table 9: Summary assessment of data-sharing mechanism in Jordan

Data-sharing mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Data classification	Open data-policy Data structure bible	• The 2017 open-data policy facilitates public access to data • The data-structure bible aims to create a common data format	• Measures are still under development • There is no common data-sensitivity framework at this time
Data exchange	Government Service Bus (GSB)	• The middleware that connects government entities across Jordan	• Uptake and use are unclear • Data exchange still appears to be occurring on a largely independent basis

2.2.2 OOP Assessment

Jordan is at a middle to high level of maturity in terms of government digitization. Though there is no data privacy or protection in place yet, the draft, which has been years in the making, is a huge step in the right direction, and some crucial advancements have been made on the data-sharing mechanism with the creation of the data-structure bible and the establishment of the GSB.

[35] Jordan E-Government Program/MOICT, "Ministry of Information and Communication Technology (MOICT) Request for Proposal," July 26, 2015, https://docplayer.net/amp/6903727-Ministry-of-information-and-communication-technology-moict-request-for-proposal-rfp-edge-enterprise-service-bus-solution.html.

At this point, implementation and uptake appear to be the primary barriers to moving forward with OOP experimentation in Jordan. Once the new Data Protection Law has been passed, the country will have all the necessary ingredients in place to adopt a principle approach to OOP and doing so may even accelerate Jordan's government digitization initiative. For more information on the OOP principle approach please refer to "Deploying the Once-Only Policy."

2.3 United Arab Emirates

Table 10: State of digital penetration in UAE

	Digital penetration in the UAE *Population: 9.83 million*	
	Number of users	Percentage of users
Internet	9.73 million	99%
Mobile	18.38 million	187%[36]
Social media	9.73 million	99%

Data Source: Various World Bank and UN reports as compiled by datareportal.com[37]

Since pivoting to a digital economy strategy in 2013, the UAE has been at the forefront of the Middle East's technological revolution. This is reflected in the impressive level of digital penetration the country has achieved (see Table 10). Today, the digital economy accounts for 4.3 percent of GDP, and it is expected that this number will continue to grow.[38]

In matters of e-government, the UAE is similarly advanced. Between 2016 and 2020, the country jumped eight positions on the UN e-government survey, and it currently ranks 21st in the world.[39] The UAE government aims to use emerging mobile technologies—such as artificial intelligence, the internet of things, and enhanced mobile security—to provide advanced services and ensure a high level of user satisfaction. It has launched several digital government transformation strategies. such as Smart Dubai 2021.[40]

2.3.1 OOP Readiness Analysis

2.3.1.1 Privacy Framework

a. Regulations

Current status: Internationally, the UAE is a signatory to several treaties with privacy implications, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Arab Charter on Human Rights.

The right to freedom and privacy of personal communications by post, telegraph, and other means are written into the UAE's constitution.

---

[36] Many residents are likely to have more than one mobile connection.
[37] "Digital 2020: The United Arab Emirates," DataReportal: Global Digital Insights, accessed August 9, 2020, https://datareportal.com/reports/digital-2020-united-arab-emirates.
[38] "Economy: The Official Portal of the UAE Government," accessed August 10, 2020, https://u.ae/en/about-the-uae/economy.
[39] United Nations Department for Economic and Social Affairs, "E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development," https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.
[40] Smart Dubai 2021, https://2021.smartdubai.ae/.

The laws in the United Arab Emirates mainland are different from those in the free zones. The mainland does not have any principal data protection legislation at the federal level.[41] Federal data protection legislation is in the works but its release date is unclear, so in its stead, data privacy and protection in areas such as communications and health are addressed via numerous sectoral regulations.

Sectoral Data-Protection Laws in the UAE

Health: A new health-data protection law was enacted in May 2019 that introduces noteworthy obligations around the collection, processing, and transfer of health data by a broad range of entities, including health-care providers, medical insurance providers, health-care IT providers, and providers of direct and/or indirect services to the health-care sector, such as outsourced services (including cloud services) located onshore.[42]

Communications: A specific law addresses the processing of telecom subscribers' data. Under powers granted to it by the 2003 Telecommunications Law, the Telecommunications Regulatory Authority has issued Consumer Protection Regulations that seek to ensure the protection of data relating to persons who contract with licensed operators for the supply of telecommunications services in the UAE,[43] including personal details, service usage details, the content of communications, account status, and payment history. Licensed operators and any third parties they are involved with are subject to a number of obligations, including taking all reasonable and appropriate measures to protect the privacy of subscriber information, whether in paper or electronic form, and preventing its unauthorized disclosure or use.

At the emirate level, Dubai has its own data law,[44] which is aimed primarily at ensuring that data gathered by Dubai government entities is effectively shared with the private sector. The Dubai Data Law conforms with international best practices, promotes transparency, and establishes rules for data dissemination, data exchange, and data sharing with nongovernmental entities. It applies to federal and local government entities that possess data relating to the Emirate of Dubai, individuals, and entities. A "competent authority" is meant to enforce the law, but who or what this refers to is unclear.

Gaps: There is no federally applicable data privacy and protection law in the UAE that governs the processing of personal data by public- or private-sector institutions, nor is there a clear-cut definition of privacy or consent. Despite this, violations of privacy are criminalized under the penal code, whose Articles 379 and 380 forbid the publishing or interception of private information.

Notably, there is significant discrepancy in the privacy framework, even at the emirate level. Dubai and Abu Dhabi have legislation, while the other six emirates are further behind on issues of privacy and broader e-government matters.

---

[41] "Law in UAE—General," Data Protection Laws of the World, DLA Piper Global, accessed August 9, 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=AE, and Rima Mrad and Nadim Bardawil, "United Arab Emirates: Data Protection 2018: UAE Chapter," Mondaq, August 10, 2020, https://www.mondaq.com/data-protection/727848/data-protection-2018-uae-chapter.

[42] Lex Arabiae, "UAE-Federal Law No. 2 of 2019 to Protect Health Data," Meyer-Reumann & Partners, https://meyer-reumann.com/latest-articles/uae-federal-law-no-2-of-2019-to-protect-health-data/.

[43] "Consumer protection," Ministry of Economy, accessed October 6, 2020, https://u.ae/en/information-and-services/justice-safety-and-the-law/consumer-protection.

[44] The Supreme Legislation Committee in the Emirate of Dubai, "Law No. 26 of 2015 Regulating Dissemination and Exchange of Data in the Emirate of Dubai," https://www.smartdubai.ae/docs/default-source/dubai-data/data-dissemination-and-exchange-in-the-emirate-of-dubai-law_2015.pdf?sfvrsn=46ac2296_6.

b. Privacy-by-design principles

Current status and gaps: Not applicable.

c. Enforcement

Current status and gaps: Not applicable.

Table 11: Summary assessment of privacy framework in the UAE

Privacy framework in the UAE			
Element	**Manifestation**	**Summary**	**Gaps**
Regulations	No federal-level data privacy and protection law exists at this time, though some sectoral and emirate-level laws are currently in place	• A draft data protection law is currently in the works.	• No federal-level law exists
Privacy-by-design principles	Not applicable		
Enforcement	Not applicable		

2.3.1.2 Identification Mechanism

Unique Identifier

Current status: All residents and citizens aged 15 and older are legally required to hold an Emirates ID, a biometrically enabled smart card linked to a 15-digit unique identifier.[45] It is the first point of interaction for government-linked transactions. Though originally envisioned as a single form of identification that will be connected to all use cases across government, many use cases have yet to be operationalized. The Federal Authority for Identity and Citizenship, which rests under the Ministry of Interior, is the primary issuing authority for the ID card.

Residents and citizens can now also apply for the UAE PASS app, the first national digital identity and signature solution in the country that enables users to: (a) identify themselves to government service providers in all emirates through smartphone-based authentication, and (b) sign documents digitally with a high level of security. By activating the UAE PASS, the user will have a single digital identity across federal and local government entities, in addition to various other service providers.

Gaps: No specific regulations have been adopted to govern the deployment of the smart ID card, and the lack of a data-protection law, as mentioned before, leaves this kind of initiative without clear regulation for the processing

[45] "Emirates ID," The Official Portal of the UAE Government, accessed August 10, 2020, https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id; "UAE Pass," Smart Dubai, accessed August 9, 2020, https://www.smartdubai.ae/apps-services/details/uae-pass; and "UAEPass User Guide: Version 1.0," https://www.mohap.gov.ae/Documents/Banner/UAEPASS_User_Guide_1.0.pdf, accessed October 18, 2020.

and security of digitized personal data. Additionally, the unique identifier on the ID is apparently not tokenized and thus seems highly exposed.

Table 12: Summary assessment of identification mechanism in UAE

Identification mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Unique identifier	Emirates ID	• All adult citizens and residents are legally required to have an Emirates ID, which is accompanied by a 15-digit unique identifier	• No legal basis for securing data linked to the smart card • National number is highly exposed

2.3.1.3 Data-Sharing Mechanism

Current status and gaps: All elements of standardized data sharing (classification and data exchange) appear to be at a nascent stage in the UAE at this time. Common data classification standards that are applied across all of government do not exist. Interdepartmental data exchange appears to occur on an ad hoc basis between individual departments and ministries with no common technology or institutional governance in place.

Streamlining services around life events in UAE

Even within the confines of the current environment, the UAE government has been experimenting with facilitating data sharing on a limited basis. For example, the federal government has been trying to streamline services by bundling them into life events such as marriage, birth, and death. The federal accelerator program facilitates streamlining by helping the relevant departments create the necessary IT structures and data-sharing arrangements needed to make the revised service work. These newly bundled services are offered on a limited scale at some kiosks across the UAE. These streamlined programs are quite similar in structure to OOP programs and can be leveraged as examples of early experimentation in this space.

Table 13: Summary assessment of data-sharing mechanism in UAE

Data-sharing mechanism			
Element	**Manifestation**	**Summary**	**Gaps**
Data classification	No standardized data-classification system is used at this time		
Data exchange	Ad hoc data exchange		

2.3.2 OOP Assessment

The UAE is far ahead of its peers in terms of government digitization. All high-priority services (approximately 10 percent of the total number of services) are digitized and available via multiple delivery channels such as apps, call centers, etc. Furthermore, the government is taking a seamless, integrated view of services while putting the customer at the center of its operations.

However, both data privacy at a federal level and data sharing are in their infancy. Today there is no data office for the government which can act as a custodian for enabling data sharing, something that anecdotally appears to be a necessary ingredient given the UAE environment. In the absence of these critical pieces the government should not embark on an OOP agenda at this time.

2.4 Overview of OOP Readiness across DAL Countries

To understand where the broader region stands in terms of OOP readiness from a principle-approach perspective (where OOP is applicable across all of government), I did a quick assessment of ten other countries. I looked specifically at whether the country had:

- data privacy and protection regulations in place, because regulations act as a proxy for the broader privacy framework.
- a leverageable national digital ID system with an accompanying unique identifier in place. Notably, though even a principle approach to OOP can technically be achieved without a digital ID system in place, it would be extremely difficult to do.

I did not look at the country's data-sharing arrangement for this assessment, as that is harder to grasp without having conversations with local experts. Instead, I have indicated where further research on the data-sharing mechanism is needed to assess OOP readiness.

Finally, it is worth mentioning that these quick assessments are only meant to give readers a sense of the current state of play. Countries interested in seriously examining their OOP readiness should conduct deeper assessments of the type shown in the sections for Lebanon, Jordan and the UAE, and consider the points raised in "Deploying the Once-Only Policy."

Table 14: Preliminary Analysis of OOP Readiness across Arab League Countries

Country	Privacy regulation	National digital ID	OOP readiness
Morocco	Yes, since 2009[46]	Yes, since 2007[47]	Further research on the country's data-sharing mechanism is required
Tunisia	Yes, since 2004[48]	No[49]	Despite a solid privacy culture, not

[46] Hind Chenaoui, "Moroccan data protection law: Moving to align with EU data protection?," Privacy Tracker, September 11, 2018, https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/.
[47] "ID4D Country Diagnostic: Morocco," World Bank, 2016, https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018-04/Morocco_ID4D_Diagnostic_Web404018.pdf.
[48] "Tunisia: Data Protection Overview," DataGuidance, April 2020, https://www.dataguidance.com/notes/tunisia-data-protection-overview.
[49] "Tunisian biometric ID programme faces privacy challenge," Security Document News, January 15, 2018, http://www.securitydocumentworld.com/article-details/i/13506/.

			ready because of the lack of a leverageable ID system
Algeria	Yes, since 2018[50]	Yes, since 2016[51]	Not ready; the privacy framework is nascent, and the Algerian Authority of Personal Data Protection has not been instituted
Egypt	Yes, since 2020[52]	No[53]	Not ready, because of a nascent privacy framework and the lack of a national-level digital ID system
Saudi Arabia	No[54]	Yes, since 2007[55]	Not ready, because of the absence of not only the framework but also of the concept of data privacy
Kuwait	No[56]	Yes, since 2009[57]	Not ready, because of the absence of not only the framework but also of the concept of data privacy
Bahrein	Yes, since 2018[58]	Yes, since 2006[59]	Further research on the country's data-sharing mechanism is required
Qatar	Yes, since 2016[60]	Yes, since 2003[61]	Further research on the country's data-sharing mechanism is required

[50] "Summary of relevant laws and regulations for investors in Algeria," Oxford Business Group, January 21, 2019, https://oxfordbusinessgroup.com/overview/legal-landscape-summary-laws-and-regulations-investors-algeria.
[51] "Algeria's new biometric identity card: a successful launch," Thales, accessed October 8, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/new-national-identity-card-algeria, and "Summary of relevant laws and regulations for investors in Algeria.
[52] PricewaterhouseCoopers, "Egypt: A New Data Privacy Law," PwC, accessed August 9, 2020, https://www.pwc.com/m1/en/services/tax/me-tax-legal-news/2019/new-egyptian-data-privacy-law-nov-2019.html.
[53] Chris Burt, "Idemia to build biometrics-backed digital identity service in Egypt, supply TSA trials, joins Kantara," Biometric Update, March 12, 2020, https://www.biometricupdate.com/202003/idemia-to-build-biometrics-backed-digital-identity-service-in-egypt-supply-tsa-trials-joins-kantara.
[54] PricewaterhouseCoopers, "Saudi Arabia: Data Privacy Landscape," PwC, accessed August 9, 2020, https://www.pwc.com/m1/en/services/tax/me-tax-legal-news/2019/saudi-arabia-data-privacy-landscape-ksa.html.
[55] "A smart national ID card for Saudi Arabia," Thales, accessed October 8, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/saudi-arabia.
[56] Data Protection Laws of the World: Kuwait," DLA Piper, accessed October 8, 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=KW.
[57] "Civil ID card in Kuwait: The key to digital government," Thales, accessed October 8, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/kuwait.
[58] "Data Protection Laws of the World: Bahrain," DLA Piper, accessed October 8, 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=BH.
[59] "New national ID card for Kingdom of Bahrain," Thales, accessed October 8, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/bahrain.
[60] "Qatar issues Personal Data Privacy Law," Ministry of Transport and Communications, November 6, 2016, https://www.motc.gov.qa/en/documents/document/qatar-issues-personal-data-privacy-law-5.
[61] "National ID cards in Qatar: from ID to digital government," accessed October 8, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-id.

Mauritania	Yes, since 2017[62]	No	Not ready because of a nascent privacy framework and the lack of a national digital ID system
Djibouti	No[63]	Yes, since 2009[64]	Not ready because of the lack of a privacy framework and a nascent digital ID program

[62] "Personal Data Protection Guidelines for Africa," Internet Society and the Commission of the African Union, May 9, 2018, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.
[63] "Privacy Is Paramount: Personal Data Protection in Africa," Deloitte, 2017, https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf.
[64] "Djibouti: Opting for Digital Identity Card," Africa Top Success (blog), August 21, 2014, https://www.africatopsuccess.com/djibouti-opting-for-digital-identity-card/.

A PUBLICATION OF THE

Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

617-495-0557
ash.harvard.edu

HARVARD Kennedy School
ASH CENTER
for Democratic Governance
and Innovation