



Jordan

Digital Trade Acceleration Initiative

Country Report

Disclaimer

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

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

This Document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Additionally, every effort was made to collect comprehensive data for this Document, which was shared with each of the DCO Member States and, through them, with relevant government agencies. The data collected was current as of September 2024, and there may have been developments or updates since that time. DCO does not undertake any responsibility for such subsequent developments or the use of data that may no longer be current.

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

DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.

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

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the Digital Cooperation Organization. The User shall not reproduce any content of this Document without obtaining DCO’s consent or shall provide a reference to DCO’s information in all cases. By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

© Digital Cooperation Organization 2025.

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

How to Read This Report

This comprehensive report is structured to guide readers to the information that interests them most. Three sections illuminate the regulatory assessment from different perspectives:

Section A is the core of this report. It assesses the domestic regulatory environment across twelve policy areas, with three subsections for each.

1. Our guiding questions analyse how each policy area interacts with digital trade.
2. Our summaries condense the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities.
3. Our source lists provide a repository of official sources to facilitate further analysis.

Section B provides a factsheet that describes the local digital economy across four key dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.

Section C outlines international commitments and references the international fora in which it engages on digital issues.

Table of Contents

01	Domestic Regulatory Environment Assessment	6
	Data Protection	8
	Cross-Border Data Transfers	11
	Location of Computing Facilities	14
	Online Consumer Protection	17
	Electronic Transactions	20
	Trade Facilitation with Digital Means	23
	Cybersecurity	26
	Artificial Intelligence	29
	Source Code	32
	Digital Economy Taxation and Customs Duties	35
	Electronic Payments	39
	SMEs and Digital Inclusion	41
02	Digital Economy Factsheet	45
	Size and Activities of the Digital Economy	46
	Digital Infrastructure and Connectivity	47
	Digital Skills	48
	Digital Government	49
03	International Commitments and Collaboration	50
	Commitments	52
	Fora	54

Executive Summary

The purpose of this report is to provide a detailed description of the regulatory environment affecting businesses and consumers engaging in digital trade. We illuminate the regulatory environment from three perspectives:

- 01 A comprehensive regulatory assessment explains the regulatory environment across twelve policy areas.
- 02 A factsheet describes the local digital economy across four dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.
- 03 An overview of existing international commitments characterises efforts to accelerate digital trade.

The regulatory assessment is the main contribution of this report and provides the following findings:

Data Protection:

The data protection law, implemented in March 2025, generally requires consent for data processing, with exceptions. Data subjects are granted rights to information, access, correction, erasure, portability, and consent withdrawal. The appointment of data protection officers is required in specific scenarios and a registry is maintained by the government.

Cross-Border Data Transfers

Cross-border data transfers are only allowed if the receiving country ensures equivalent data protection. The government is to issue a list of countries that provide sufficient data protection. Transfers to other countries are only allowed in specific exceptions, including when the data subject consents, for international cooperation, or for medical purposes.

Location of computing facilities:

Jordan does not generally require data to be localised. Specific data localisation mandates apply to government data of a secret or sensitive nature.

Online Consumer Protection:

Online consumers are protected by the general consumer protection framework, which prohibits making misrepresentations. Licensed entities can send four types of bulk messages (Advertisements, Alerts, Awareness, Services).

Electronic Transactions:

Electronic transactions are allowed and electronically signed documents are granted the same legal effect as paper-based equivalents, if the electronic signature comprises certain characteristics. Jordan distinguishes between “protected” and “authenticated” electronic signatures.



01

Domestic Regulatory Environment Assessment

Domestic Regulatory Environment Assessment

For thriving digital trade among the members of the Digital Cooperation Organization, their regulatory environment should be comprehensive and adaptive. Absence of fundamental regulatory building blocs, regulatory divergence, or explicit barriers can hinder the DCO Member State's digital trade reaching its potential.

This section assesses the regulatory environment across twelve policy areas on three layers. First, we answer guiding questions to analyse each policy area's impact on digital trade. Second, we summarise the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities. Third, we provide a repository of official sources to facilitate further analysis.

We conduct this assessment for the following policy areas:

- 01 Data Protection
- 02 Cross-Border Data Transfers
- 03 Location of Computing Facilities
- 04 Online Consumer Protection
- 05 Electronic Transactions
- 06 Trade Facilitation with Digital Means
- 07 Cybersecurity
- 08 Artificial Intelligence
- 09 Source Code
- 10 Digital Economy Taxation and Customs Duties
- 11 Electronic Payments
- 12 SMEs and Digital Inclusion



Data Protection

The purpose of this section is to comprehensively characterise the conditions for domestic data collection and processing. Alignment with international best practices in data protection is important for fostering trust whilst facilitating market access. Deviation from these practices could potentially impact digital trade. If the data protection requirements within the member state are too low, that diminishes trust. If data protection requirements are too high, that may delay market entry from international service providers.

Guiding Questions

We analyse whether user consent is required for the processing of personal data. We then delineate the rights of data subjects and obligations for those processing data, specifically on local representation and registration. Finally, we identify the authority responsible for overseeing and enforcing data protection regulations.

Jordan's data protection law, which is in force with a grace period until March 2025, generally requires consent for data processing. It foresees exceptions, such as data processing for the protection of vital interests and compliance with legal obligations. Data subjects are granted rights to information, access, correction, erasure, portability, and consent withdrawal. The appointment of data protection officers is required in specific scenarios (outlined below) and a registry of controllers, processors, and data protection officers is maintained by the government. The Personal Data Protection Council under the Ministry of Digital Economy and Entrepreneurship oversees data protection, along with sectoral bodies.

Summary

- Jordan's Personal Data Protection Law, in force since March 2024, will be fully implemented by March 2025. The law applies to any natural or legal person, who has data under their custody.
- It mandates that the data subjects provide written consent for data processing and grants them the rights to information, access, consent withdrawal, rectification, and objection to the processing of their data. The Law requires data controllers to appoint data protection officers in specific scenarios, including if data processing is the controller's primary activity and if the controller processes sensitive personal data, financial information, data of individuals without legal capacity, or if the controller transfers databases abroad.
- The Law further tasks the Ministry of Digital Economy and Entrepreneurship to establish a registry of data controllers, data processors, and data protection officers, on which instructions were published for consultation in February 2024.
- The Law further states that a Personal Data Protection Council and Unit are to be established (under the Ministry of Digital Economy and Entrepreneurship) to oversee data protection. The Council will be responsible for setting policies, adopting standards, issuing licences, and reviewing complaints.
- The Council may also impose penalties based on the recommendations of the Personal Data Protection Unit. In addition, the Central Bank of Jordan is responsible for implementing the Credit Information Law and its related regulations.



- The Ministry of Digital Economy and Entrepreneurship published four draft regulations and three draft instructions for consultation in February 2024. The draft regulations cover licences and permits, data disclosure, mechanisms and procedures for the work of the unit, data subject rights and procedures for prior consent and withdrawal. The draft instructions address security, technical and regulatory measures, the personal data protection registry, and the personal data protection council.
- The Ministry of Digital Economy and Entrepreneurship further issued the Internet Safety Guidelines, which include safety instructions for internet use by internet providers, users (parents and children), and e-commerce providers such as not disclosing personal information or entering sensitive data or pictures when using public internet connections.



SOURCES

Primary Legislation

- The Personal Data Protection Law No. 24 for the year 2023
- The Credit Information Law No. 15 for the year 2010

Secondary Legislation

- Ministry of Digital Economy and Entrepreneurship: Draft Regulation on Data Disclosure
- Ministry of Digital Economy and Entrepreneurship: Draft Regulation on Mechanisms and Procedures of the Unit
- Ministry of Digital Economy and Entrepreneurship: Draft Regulation on Licences and Authorisations
- Ministry of Digital Economy and Entrepreneurship: Draft Instructions on Security, Technical, and Regulatory Measures
- Ministry of Digital Economy and Entrepreneurship: Draft Instructions on Personal Data Protection Registry
- Ministry of Digital Economy and Entrepreneurship: Draft Instructions on Personal Data Protection Council
- Central bank of Jordan: Bylaw of Credit Information Companies no (36) of the Year (2011)
- Central Bank of Jordan: Instructions on Business Controls for Credit Information Companies no (13/ 2022)

Guidelines

- Ministry of Digital Economy and Entrepreneurship: Internet Safety Guidelines

Oversight Authorities

- Ministry of Digital Economy and Entrepreneurship
- Central Bank of Jordan



Cross-Border Data Transfers

The purpose of this section is to analyse the conditions for the cross-border transfer of personal information. On the one hand, data flows are the bloodline of the digital economy. On the other hand, data flows are a controversial subject in geopolitical discussions, as governments worry that transferring data across borders may jeopardise its protection. How a government regulates data transfers reveals the balancing act between free data flows and protection of data abroad.

Guiding Questions

We differentiate whether the framework treats cross-border transfers differently from in-country transfers. We then analyse the specific conditions for cross-border transfers, ranging from data subject consent, to governmental adequacy decisions, to certification and contractual mechanisms. Finally, we delineate conditions for specific types of cross-border transfers and distil public policy objectives invoked by the government, where explicitly stated.

Cross-border data transfers in Jordan are subject to specific rules. They are generally prohibited, unless the receiving country or organisation ensures equivalent data protection. The government is responsible for issuing a list of countries, entities, and international organisations that provide sufficient data protection. Transfers to other countries are only allowed in specific exceptions, including when the data subject consents, for international cooperation, or for medical purposes. There are no specific conditions for transfers based on certain data types.

Summary

- The Personal Data Protection Law, which is in force since March 2024 and will be fully implemented in March 2025, establishes specific rules for cross-border data transfers. Data transfers are generally prohibited unless the receiving country or organisation ensures data protection standards that align with Jordanian law. Before transferring data, data controllers must verify the level of protection provided by the recipient to ensure the security of the Data. The Personal Data Protection Council is tasked with issuing a list of countries, entities, and international organisations that provide a sufficient level of data protection.



Transfers to other countries, without a sufficient level of data protection, are only allowed in specific exceptions, including:

- 01 cooperation under international agreements or treaties.
- 02 cooperation to combat crimes and pursue criminals.
- 03 exchange of medical data necessary for the treatment of the data subject.
- 04 exchange of data related to public health.
- 05 transfers of funds outside the Kingdom.
- 06 data transfers to which the data subject has consented, after receiving information that there is an insufficient level of protection at the destination of the transfer.

SOURCES

Primary Legislation

- The Personal Data Protection Law No 24 for the year 2023r



Location of Computing Facilities

The purpose of this section is to crystallise instances in which data must be stored in local computing facilities. Data localisation mandates require foreign providers to invest in or rent local infrastructure. This can create a significant barrier to digital trade due to burdensome procedural requirements or costs. Such requirements are thus subject to international scrutiny regarding their justification and scope.

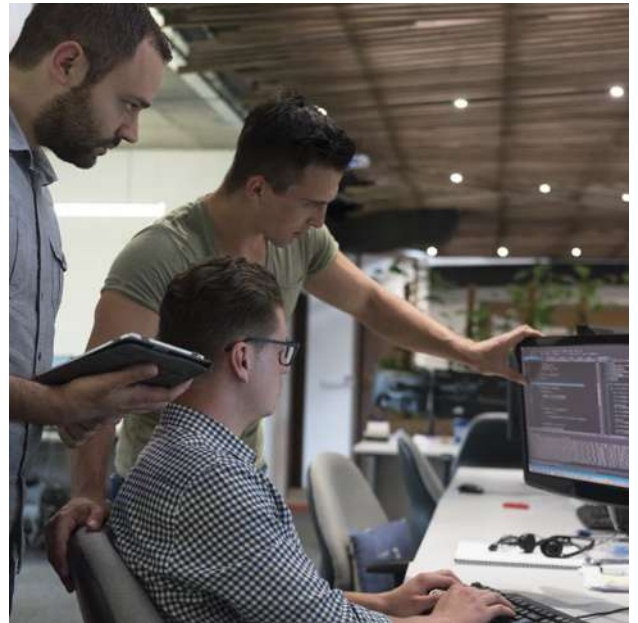
Guiding Questions

We analyse whether the framework generally requires data to be stored in the national territory. We then analyse whether data localisation requirements apply to specific data types, such as infrastructure or health data. For each identified localisation requirement, we distil the public policy objective invoked by the government, if it is explicitly stated.

Jordan does not generally require data to be localised. Specific data localisation mandates apply to government data. Specifically, the Cloud (Platforms and Services) Policy includes that government data is classified into four levels (secret, sensitive, private, and ordinary data) and secret and sensitive data must be stored in Jordan.

Summary

- There is no general data localisation mandate in Jordan, although specific government data must be stored in Jordan. The Cloud (Platforms and Services) Policy applies to all government entities and all cloud services providers, seeking to develop an integrated cloud ecosystem through government use of cloud services, among other objectives. The Policy requires government agencies to classify their data, equipment, and software, which is to be transferred to the cloud, in accordance with the Data Classification and Management Policy of 2020. Data is classified into four levels: secret, sensitive, private, and ordinary data. Secret and sensitive data storage and processing must occur in Jordan, specifically in secure data centres within the government that offer the possibility of restrictions.





SOURCES

- The Personal Data Protection Law No 24 for the year 2023
- Cloud (Platforms and Services) Policy 2020
- Government Data Classification and Management Policy, 2020



Online Consumer Protection

This section provides a detailed overview of the approach to protecting online consumers. A well-regulated online consumer protection framework is crucial for fostering trust and confidence in online transactions. In the context of international trade, the implementation of strong online consumer protection regulations enables secure cross-border transactions and promotes the expansion of e-commerce.

Guiding Questions

We contour whether the online consumer protection framework is specific to online consumption or applies general rules thereto. We then delineate the practices that are considered violations of consumer protection and distil any special obligations for e-commerce platforms. We further analyse the regulatory approach regarding spam. Finally, we explain which authority oversees online consumer protection.

Online consumers are protected by the general consumer protection framework, mainly the consumer protection law. The law prohibits practices including making misrepresentations and failing to provide goods or services that do not conform to declared characteristics. E-commerce platforms are not subject to specific indirect obligations. Licensed entities can send four types of bulk messages (Advertisements, Alerts, Awareness, Services). The Consumer Protection Council, chaired by the Minister of Industry, Trade and Supply, is in charge of oversight and resolved 94% of the 820 complaints received in 2023.

Summary

- The Consumer Protection Law was enacted in 2017.

The law establishes consumer rights including obtaining full and accurate information on the product or service bought, the terms of the sale, and the provider address, as well as the right to compensation. The law also establishes provider obligations, such as ensuring quality and compliance, delivering as agreed, and not violating intellectual property rights. The law also includes after-sale provisions regarding returns and compensation for defective products and services.

- The law established a Consumer Protection Council chaired by the Minister of Industry, Trade and Supply. It includes representatives from both the public and private sectors. The Council reports directly to the Council of Ministers and can formulate and advise on consumer protection policy. Additionally, the law created a Consumer Protection Directorate within the Ministry of Industry, Trade and Supply. This directorate oversees the implementation of the law, manages consumer and association complaints, documents violations, and forwards complaints to the relevant agencies.

- The Consumer Protection Instructions were issued in the year 2023, specifying the provisions of the Consumer Protection Law.

Other agencies have also issued secondary legislations:

- 01 The Telecommunications Regulatory Commission issued instructions that regulate the sending of wholesale messages, aiming to control and mitigate the impact of spam messages on consumers. The Telecommunications Regulatory Commission is further responsible for consumer complaints for e-commerce and issues licenses for postal services. In 2024, an instruction outlined that four types of bulk messages (Advertisements, Alerts, Awareness, Services) can be sent, although only by licensed entities. Senders must further establish cybersecurity protections.
- 02 The Ministry of Industry, Trade and Supply issued the Consumer Protection Guide. The guide was developed in 2022 and includes elaboration of consumer rights, provider commitments and obligations, complaints` channels and resolution, and penalties.
- 03 The Civil Aviation Regulatory Commission issued the Civil Aviation-Consumer Protection Instructions of 2020.
- 04 The Central Bank issued Instructions on Financial Consumer Protection for Electronic Money Payments and Transfers, Microfinance Sector, and for Licensed Exchange Companies`s Clients.



SOURCES

Primary Legislation

- Consumer Protection Law No. 7 for the year 2017

Secondary Legislation

- Consumer Protection Instructions for the year 2023
- Telecommunications regulatory Commission: Instructions on Sending Wholesale Messages
- Civil Aviation Consumer Protection Instructions, 2020
- Financial Consumer Protection for Electronic Money Payments and Transfers
- Instructions on Financial Consumer Protection for Microfinance Sector
- Instructions on Financial Consumer Protection for Licensed Exchange Companies`s Clients.

Guidelines

- Consumer Protection Guide

Oversight Authorities

- Ministry of Industry, Trade and Supply
- Civil Aviation Regulatory Commission



Electronic Transactions

The purpose of this section is to identify whether there are any regulatory hurdles to electronic transactions compared to paper-based or face-to-face transactions of equivalent substance. A transaction contains different aspects such as the validity of the contract, signature, and authentication.

Guiding Questions

We focus on whether the electronic transactions framework is binding and whether it recognises electronic transactions as equivalent to paper-based transactions. We then differentiate the various types of electronic signatures in the framework. Finally, we distil whether electronic authentication is permitted and whether the government provides such authentication.

Electronic transactions are governed by a dedicated law which grants electronic documents, records, and contracts the same legal effect as paper-based equivalents. Exceptions are foreseen for transactions regarding civil status and contracts regarding real estate. The framework grants validity to electronic signatures, differentiating between protected electronic signatures and authenticated electronic signatures. Electronic authentication is accepted and the government provides electronic authentication through a digital ID application (Sanad).

Summary

- The Electronic Transactions Law, in force since 2015, grants electronic documents, records, and contracts the same legal effect as paper-based documents, with exceptions for transactions related to movable and immovable property, civil status, utilities, and health and life insurance. Electronic transactions are legally valid if the electronic record information is accessible and can be stored and referenced without any modifications.
- The framework distinguishes between protected and authenticated electronic signatures. Electronic signatures are considered to be “protected” and thus legally binding based on the following characteristics: The signatory is uniquely identifiable, the private key is controlled by the signatory at the time of signing, and the signature is associated with the electronic record in a way that prevents any changes without altering the signature.
- An electronic signature is considered “authenticated” if it is linked to an electronic authentication certificate issued by a licensed electronic authentication body, an accredited electronic authentication body, or a dedicated government entity. The Ministry of Digital Economy and Entrepreneurship is the electronic documentation body for ministries, public institutions, and municipalities. Sectoral regulators issue documentation in their domains, for example the Central Bank of Jordan with regard to electronic banking or financial business.



- An electronic record linked to a protected electronic signature holds the same legal authority as an ordinary document. When an electronic record is associated with an authenticated electronic signature, it holds the same legal authority as an ordinary document, and both the contract parties and third parties can rely on it. An electronic record without an electronic signature has the same legal standing as an unsigned paper document.
- The framework also allows for the licensing of authentication bodies in the private sector. The Telecommunications Regulatory Commission issued the Licensing and Accrediting Bodies for Electronic Authentication Bylaw in 2014 (amended in 2016). This bylaw includes instructions on licensing, accrediting, and monitoring certification authorities, as well as provisions for the suspension or cancellation of licences for certification authorities.
- Finally, the Ministry of Digital Economy and Entrepreneurship developed a mobile application called “Sanad” which is the government application providing digital ID and other government services.



SOURCES

Primary Legislation

- Electronic Transactions Law no. 15 for the year 2015

Secondary Legislation

- Telecommunications Regulatory Commission: Licensing and accrediting bodies for electronic authentication bylaw, 2014
- Telecommunications Regulatory Commission: Amended in 2016 Licensing and accrediting bodies for electronic authentication bylaw
- Telecommunications Regulatory Commission: Instructions on Licensing and accrediting bodies for electronic authentication
- Telecommunications Regulatory Commission: Instructions for cancellation or suspension of licence and accreditation for certification authorities
- Telecommunications Regulatory Commission: Authorised certification authorities supervision instructions
- Telecommunications Regulatory Commission: Instructions on monitoring certification authorities
- Telecommunications Regulatory Commission: Instructions on auditing certification authorities

Guidelines

- Sanad Application
- Central Bank of Jordan: National Strategy for Electronic Payments in Jordan (2023-2025)



Trade Facilitation with Digital Means

This section analyses how well the domestic regulatory environment is set up to welcome goods and services trade made possible through digital tools. This includes the use of electronic trade documentation, as well as measures designed to support "trade in parcels" and streamline cross-border transactions in the digital economy.

Guiding Questions

We analyse whether trade administration documents for imports are available and can be submitted in electronic form. We then focus on single windows, enabling persons to submit documentation for import, export, or transit through a single entry point to authorities. Specifically, we outline whether a single window system is operational for trade documentation and whether this system supports international data or document exchange. Finally, we highlight expedited or simplified customs procedures for low-value shipments.

Jordan provides trade administration documents for imports in electronic form and enables electronic submission. The Jordan Customs ASYCUDA Portal serves as an integrated customs management system, facilitating trade. Jordan has established a National Single Window to facilitate trade and customs clearance processes. To enhance cross-border customs collaboration, Jordan has established electronic information exchanges with other countries. Simplified customs procedures apply to shipments valued below JOD 200.

Summary

- Jordan has taken steps to modernise its trade and customs processes through the implementation of paperless trade systems. According to the Customs Law 1998, electronic documents are equal to physical documents to facilitate trade documents processing and expediting shipments. Additionally, the Electronic Transactions Law 2015 facilitates the use of electronic signatures and documents, which is crucial for the functioning of paperless trade. Jordan has established a National Single Window to facilitate trade and customs clearance processes. The system is designed to enable businesses and traders to submit customs declarations and supporting documents electronically. By consolidating interactions with various border agencies, the NSW aims to streamline procedures, reduce delays, and promote efficiency in cross-border trade. There is currently no public, official online source available to access the National Single Window.
- Jordan has strengthened cross-border customs collaboration with several Arab countries. It has established electronic information interchange and data exchange with Saudi Arabia, Syria, Egypt, Tunisia, Morocco, and Palestine. Through its national strategies and visions, Jordan places a strong emphasis on digitizing trade processes, streamlining customs procedures, and fostering regional collaboration. These initiatives bolster the logistics, transportation, and express postal sectors, to meet the growing demands of e-commerce and advance the digital trade ecosystem.



- The Jordan Trade Portal serves as an online platform where traders can access information on trade procedures, tariffs, and regulatory requirements. The portal is designed to be a one-stop-shop for all trade-related information, providing transparency.
- In September 2024, Jordan Customs, in collaboration with Jordan Post, launched the e-commerce customs centre to expedite the clearance of incoming online shipments.
- Jordan's customs duties on postal parcels for personal use are set at a unified fee of 10% of the parcel's value, with a minimum charge of 5 dinars, for parcels valued up to 200 Jordanian dinars. Parcels are exempt from additional taxes, including the general sales tax, and do not require a formal customs declaration. A risk assessment methodology is in place to limit manual inspections. Exceptions to these reforms include tobacco products, alcoholic beverages, and parcels arriving in commercial quantities.



SOURCES

Primary Legislation

- Customs Law No. (20) for the year 1998 as amended
- Electronic Transactions Law no. 15 for the year 2015

Secondary Legislation

- Ministry of Finance Decisions

Guidelines

- Jordan Customs ASYCUDA Portal
- Jordan Trade Portal
- Decision on Establishment of the E-Commerce Customs Centre [third party source]
- National Single Window [no source available]
- News report: The E-Commerce Customs Centre becomes Operational [third party source]



Cybersecurity

This section aims to assess whether the cybersecurity requirements of the member state broadly align with international best practices. While cybersecurity is a critical component of digital policy, its relevance to digital trade is limited. Cybersecurity primarily concerns national defence, critical infrastructure, cybercrime prevention, and system integrity. However, alignment with international cybersecurity standards is essential for creating a secure environment conducive to digital trade. Insufficient cybersecurity standards can undermine trust, while overly stringent requirements may hinder market entry for international service providers.

Guiding Questions

We outline whether there is a regulatory framework regarding cybersecurity. We explain whether this framework is risk-based, creating tiered obligations depending on the extent of cybersecurity risk. We then analyse whether and to whom incident notification is required. Finally, we explain which authority oversees cybersecurity.

The cybersecurity framework comprises laws on cybersecurity and cybercrimes. Obligations are not risk-based, though penalties vary according to the severity of violations. Any incident that threatens cybersecurity must be notified to the National Cyber Security centre. In addition, the Personal Data Protection Law requires data breaches to be notified to the data subject and the Personal Data Protection Unit. The National Cyber Security centre is responsible for oversight.

Summary

- The main laws regulating cybersecurity in Jordan are the Cyber Security Law 2019 and the Cyber Crimes Law 2023. The Cyber Security Law establishes the governance structure for cybersecurity, while the Cyber Crimes Law outlines cybersecurity violations and corresponding penalties. Violations include unauthorised access to networks or databases with the intent to cancel, delete, republish, or change the content or functionality of databases or websites. In addition, the Personal Data Protection Law requires personal data breaches to be notified to the data subject within 24 hours and to the National Cyber Security Centre within 72 hours.
- The draft 2022 Cyber Security Services Providers Licensing Regulation, issued pursuant to the Cyber Security Law, regulates the licensing procedures and requirements for service providers and includes that instructions will be issued to elaborate on the licensing. The final regulation distinguishes nine services and plans to introduce an instruction and roadmap for each of the nine services in the coming years.
- The National Cyber Security centre, established under the Cyber Security Law, is responsible for overseeing cybersecurity in Jordan and handles cybersecurity complaints. Any incident that threatens cybersecurity must be notified to the National Cyber Security centre. The law further grants designated employees judicial powers to refer violations to public prosecution or the competent court. Additionally, the law established a National Cyber Security Council for approving policies and strategies related to cybersecurity. The

Council's duties include drafting policies, licensing cybersecurity services providers, and supporting public and private agencies. Current priorities of the National Cyber Security Centre include certification and developing a cybersecurity product acquisition policy, which serves as a step towards accreditation by the CCRA, of which Jordan is an official member.

Several agencies have issued secondary legislation and guidance regarding cybersecurity:

- 01 The National Cyber Security Centre issued the Cyber Security Services Providers Licensing Regulation 2022 and the Cybersecurity Incidents Classification Instructions 2023. The centre further developed the Framework Policy for Data Security in 2018, the Government's Cybersecurity Products Acquisition Policy 2023, and the Cybersecurity Framework Booklet.
- 02 The Ministry of Digital Economy and Entrepreneurship issued the National Cyber Security Strategy 2018-2023 (a new strategy for the 2024-2028 period was launched recently but not yet published), the Cybersecurity Risk Management Policy 2019, the Cybersecurity Clearance Policy 2019, and the Cybersecurity Information Security Policy 2019.
- 03 The Central Bank of Jordan developed the Cybersecurity Framework for Jordan Financial Sector in 2021, and the Instructions for Cyber Risks Resilience.



SOURCES

Primary Legislation

- Cyber Security Law No. 16 for the year 2019
- Cyber Crimes Law No. 17 for the year 2023
- The Personal Data Protection Law No 24 for the year 2023

Secondary Legislation

- National Cybersecurity Centre Regulation, 2022
- Cybersecurity Services Providers Licensing Regulation for the year 2022
- Cybersecurity Incidents Classification Instructions for the year 2023
- Instructions for Cyber Risks Resilience.

Guidelines

- National Cyber Security Centre: Framework Policy for Data Security, 2018
- National Cyber Security Centre: Government's Cybersecurity Products Acquisition Policy, 2023
- National Cyber Security Centre: Cybersecurity Framework Booklet
- Ministry of Digital Economy and Entrepreneurship: National Cybersecurity Strategy 2018-2023
- Ministry of Digital Economy and Entrepreneurship: Cybersecurity Risk Management policy 2019
- Ministry of Digital Economy and Entrepreneurship: Cybersecurity Clearance Policy 2019
- Ministry of Digital Economy and Entrepreneurship: Cybersecurity Information Security Policy 2019
- Central Bank of Jordan: Cybersecurity Framework for Jordan Financial Sector, 2021

Oversight Authorities

- National Cyber Security Centre
- Ministry of Digital Economy and Entrepreneurship
- Central Bank of Jordan



Artificial Intelligence

This section offers an overview of how artificial intelligence (AI) is regulated in the member state. The focus is on the policy response to the rise of widely accessible AI, covering both AI-specific regulatory frameworks and the application of existing laws to AI technologies. From a digital trade perspective, the key consideration is whether the member state aligns with emerging international practices.

Guiding Questions

We outline whether there is a specific regulatory framework addressing AI. If so, we analyse whether the framework is risk-based, meaning it establishes obligations based on the level of AI risk. We also analyse whether the framework is technology-based, meaning it establishes rules based on specific AI technologies. Finally, we reference guidance released by regulatory agencies on how the existing, non-AI-specific framework, applies to AI providers.

There is currently no specific regulatory framework on the governance of AI. Accordingly, neither risk-based nor technology-based obligations are imposed on AI providers. The government has issued several non-binding frameworks on AI, including the 2020 AI Policy, the 2023-2027 AI Strategy, and the National AI Code of Ethics. No regulatory agencies have issued guidelines on how existing rules apply to AI providers.

Summary

There is currently no primary or secondary legislation related to AI.

○ The Ministry of Digital Economy and Entrepreneurship developed the AI Policy in 2020 which includes 5 pillars: governance, legislative and regulatory environment, digital infrastructure, business and investment environment, and capacity building. The policy identifies the application of AI in the public sector as a government priority. Its goals are to enhance the efficiency of government services, support the local AI ecosystem, build public trust in government services, foster a culture of openness to AI, and stimulate investment in key areas such as health, education, energy and clean technology, financial services, transportation, telecommunications, and cybersecurity. Additionally, the policy seeks to promote AI adoption and development in the private sector. This effort aims to solidify Jordan's status as a leading regional IT research and entrepreneurship hub, and to boost the contribution of the information and communication technology sector to the Jordanian economy.

○ The Ministry of Digital Economy and Entrepreneurship then developed the AI Strategy for the years 2023-2027. The Strategy features 68 projects aiming to position Jordan as a regional leader in AI and to foster technological innovation and entrepreneurship. The National Council for Entrepreneurship through the Ministry of Digital Economy and Entrepreneurship oversees the implementation of the AI Strategy in Jordan. The National Council formed a Directorate on AI and a steering committee for this purpose. It reports to the Council of Ministers on the implementation of the AI Strategy.



○ The Ministry of Digital Economy and Entrepreneurship also developed the National AI Code of Ethics to achieve the desired benefit from AI applications without compromising basic human rights. The Code was developed in line with the UNESCO Recommendation on the Ethics of Artificial Intelligence.

SOURCES

Guidelines

- Artificial Intelligence Policy, 2020
- Artificial Intelligence Strategy, 2023-2027
- National AI Code of Ethics

Oversight Authorities

- Ministry of Digital Economy and Entrepreneurship



Source Code

Source codes are among the essential trade secrets of the digital economy. Potential disclosure requirements toward the government or domestic private companies can be a major hurdle to market access. The purpose of this section is to identify regulatory or enforcement requirements that risk the required disclosure of source code.

Guiding Questions

We explain whether source code is generally protected under the intellectual property framework and whether there are exceptions to this protection. We then identify potential source code sharing requirements, explaining the circumstance and specific software to which they apply. Where explicitly stated, we reference the public policy objective invoked by the government.

The copyright law provides protection to computer programs in the origin or machine language. Protection provides the copyright author with exclusive rights to exploit the work, as well as to attribution and challenging infringements, among others. The law establishes exceptions for the use of published works without the author's permission, for example in personal settings, as well as the copy of work without author's consent, for archival purposes. Jordan does not mandate any form of source code sharing.

Summary

- The Copyright Protection Law protects computer programs, whether in the origin language or machine language, as works created in literature, art, and science. For a 50 year protection period, the author retains rights to exploit their work as well as exclusive rights to have the work attributed to them with their name cited on all reproductions; make alterations, including modifications, edits, omissions, or additions; challenge infringements and prevent distortion or modification; and withdraw the work from circulation for legitimate reasons, provided they fairly compensate the holder of the monetary rights.
- The protection is subject to several exceptions. Published works can be used for presentations and exhibitions, employed for private personal use (including by making a copy), as well as for illustration in education. In addition, a copy of the work for archival purposes is allowed without the author's consent, including under the National Library Department's Deposit Centre.



SOURCES

Primary Legislation

- The Copyright Protection Law No. 22 for the year 1992 and its amendments

Secondary Legislation

- Deposit Regulations No. (4) of 1994



Digital Economy Taxation and Customs Duties

The purpose of this section is to identify how the digital economy is taxed domestically and at the border. This covers direct taxes, indirect taxes, and customs duties, applicable to both digital services/products and e-commerce imports. We focus on whether a) requirements are applied identically to digital services/products as to their analog equivalents and b) requirements are applied identically to domestic and foreign suppliers.

Guiding Questions

We explain whether customs duties apply to digital services/products as well as e-commerce imports. We then analyse whether indirect taxes, such as value-added-tax, apply to digital services/products as well as e-commerce imports. In addition, we identify any direct taxes imposed specifically on providers of digital services/products, such as digital service taxes. For each tax or duty, we mention whether electronic registration is possible for foreign providers.

Digital services or products are not subject to customs duties but are subject to the general sales tax. E-commerce imports are subject to general sales tax and customs duties, if they are valued more than JOD 200, reduced duties apply for imports valued less. The general sales tax applies for service providers if their yearly sales exceed JOD 30000 and for product providers if their yearly sales exceed JOD 75000. Jordan has not adopted specific direct taxes targeting digital providers. Electronic tax registration is possible electronically, through a dedicated portal for foreign e-commerce providers.

Summary

- The Customs Law applies to products physically imported into Jordan, including e-commerce imports but excluding digital services. E-commerce imports valued below JOD 200 are subject to a reduced customs duty of 10%, albeit with a minimum duty of JOD 5. Shipments valued above JOD 200 are subject to normal customs requirements and rates.
- The General Sales Tax is applied on all products and services consumed in the local market. A threshold exists for providers to register for GST, namely if yearly sales exceed JOD 30000 for services or JOD 75000 for products. Providers must collect the GST and transfer the amounts collected periodically to the Income and Sales Tax Department, which oversees the implementation of the General Sales Tax Law.
- The Income and Sales Tax Department, under the Ministry of Finance, developed a portal for the registration of non-resident e-commerce providers in 2024. Jordan also provides income tax exemptions for the ICT sector and services exports.



SOURCES

Primary Legislation

- Customs Law No. (20) for the year 1998 as amended
- General Sales Tax Law for the year 1994 and its amendments

Secondary Legislation

- Ministry of Finance Decisions

Guidelines

- Income and Sales Tax Department: Thresholds for GST registration
- Income and Sales Tax Department: Platform of the General Tax on Ecommerce Sales for Non-Residents



Electronic Payments

This section evaluates the key aspects of the regulatory environment governing electronic payments and its openness to processing payments across borders. Electronic payments are a critical enabler of digital and digitally facilitated trade. While data protection, data flows, and electronic transactions play a significant role in electronic payments, they have been addressed previously. This section focuses on whether a) digital payment services/products are subject to the same requirements as their analogue equivalents, and b) whether these requirements are applied equally to domestic and foreign providers.

Guiding Questions

We outline whether there is a regulatory framework specifically addressing electronic payments. We then distil know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to electronic payments. In addition, we delineate licensing requirements and procedures for entities that offer electronic payment services. Finally, we reference special regulatory requirements for cross-border electronic payments.

Electronic payments are governed by both general rules on the provision of payment services and specific rules for electronic payments. Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules, enshrined in the Anti Money Laundering and Counter Terrorist Financing Law, apply to electronic payment providers. Electronic payment providers must further obtain a licence from the central bank, according to the Bylaw of Electronic Payment and Money Transfer.

Summary

- The Bylaw of Electronic Payment and Money Transfer, issued pursuant to the Electronic Transactions Law, was enacted in 2017 to regulate the electronic payments. The Central Bank of Jordan is mandated with its implementation. The Bylaw requires that any payment services provider should get a licence from the Central Bank and includes the process and requirements for the licence. Foreign companies can deliver payment services via a local branch.
- The Central Bank also developed the Instructions for Regulating Know your Customer Procedures and dealing with customers electronically pursuant to the said regulations which apply to banks and companies providing payment services and does not apply to exchange companies. These instructions shall be applied when establishing a remote banking or business relationship with natural persons only as a first stage, provided that this is allowed for legal persons at a later stage according to a notice issued by the Central Bank in this regard. Jordan further provides an eKYC system to facilitate compliance.
- The Anti Money Laundering and Counter Terrorist Financing Law, as well as its regulations and instructions, establish obligations for banks, financial companies, and insurance companies. Any financial activities that exceed JOD 10000 or an equivalent amount in foreign currency must be registered. Entities must further perform due diligence to verify the identity of the customer, their legal status, business activities, the purpose and nature of the relationship, and the beneficial owner. Due diligence includes detailed verification and continuous monitoring of transactions in ongoing customer relationships. Additionally, the nature and

purpose of the future relationship with the customer must be identified, with related data recorded and maintained as per the relevant provisions. The Law is implemented by the Anti Money Laundering and Counter Terrorist Financing Unit.

- The payment services or the operation and management of the e-payment systems cannot be exercised unless the licence required has been obtained from the Central Bank. Among the licence requirements is to prepare plans and programs of the company in terms of anti-money laundering and counter funding of terrorism as well as the mechanism of dealing with customers and processing their complaints.

The following guidelines were developed to assist companies in compliance with relevant regulations:

- 01 Guidelines of Anti Money Laundering and Counter Terrorist Financing Transactions for Entities Exercising any of the Financial Activities.
- 02 Licensing Guideline For Electronic Payments & Money Transfer Activities for local companies and branches of foreign companies.
- 03 To improve digital financial inclusion, the National Strategy for E-Payments (2023-25) aims to improve systems including the CLtIQ instant payment system.



SOURCES

Primary Legislation

- Central Bank of Jordan: Bylaw of Electronic Payment and Money Transfer No. (111) for 2017
- Anti-Money laundering Unit: Anti Money Laundering and Counter Terrorist Financing Law No. (20) of 2021

Secondary Legislation

- Central Bank of Jordan: Instructions for Regulating Know your Customer Procedures and dealing with him electronically NO. (7/2021)
- Anti-Money Laundering Unit: Instructions No. (3) for the year 2011 Anti Money Laundering and Counter Terrorist Financing Instructions For Entities Exercising any of the Financial Activities

Guidelines

- Anti-Money Laundering Unit: Guidelines of Anti Money Laundering and Counter Terrorist Financing Transactions for Entities Exercising any of the Financial Activities
- Central Bank of Jordan: Licensing Guideline For Electronic Payments & Money Transfer Activities



SMEs and Digital Inclusion

Digital trade holds the potential to open global markets to SMEs and disadvantaged groups. By leveraging digital technologies, small businesses, rural enterprises, and minority-owned businesses can overcome traditional barriers to international trade, such as high costs, limited market access, and logistical challenges. E-commerce platforms, digital payment systems, and online marketing tools enable these businesses to reach international customers, integrate into global value chains, and attain economies of scale previously limited to larger corporations. This section highlights recent support measures targeted to helping SMEs and disadvantaged groups capitalise specifically on the opportunities of the global digital economy.

Guiding Questions

We analyse whether the government has established specific programs or initiatives to support SMEs or disadvantaged groups in participating in the digital economy or digital trade. For each program, we distil the objective of the support, the form of support provided, and the target group of the program.

Jordan has implemented a range of initiatives to support SMEs and disadvantaged groups in accessing digital trade opportunities. These efforts include national strategies that prioritise digital transformation and e-commerce, government-led programmes offering technical and financial support, and specialised initiatives targeting women entrepreneurs. The measures span from broad policy frameworks to targeted assistance programmes, aiming to enhance the digital capabilities and market access of Jordanian SMEs.

Summary

○ The Jordanian government has established several strategic frameworks to guide the digital inclusion of SMEs. The Reach 25 National Vision & Strategy sets out objectives for developing a competitive digital economy by 2025, emphasising SME support and digital skills development. Jordan's Vision 2025 and the associated Digital Transformation Strategy and Implementation Plan 2021–2025 incorporate provisions specifically addressing SMEs in the digital economy. Additionally, the 2023 National E-Commerce Strategy identifies enhancing SME competitiveness through e-commerce solutions and modern technologies as a key objective for 2023-2025.

○ The Jordan Enterprise Development Corporation (JEDCO) plays a central role in supporting SMEs' digital integration. JEDCO's strategic plan for 2022-2025 prioritises enhancing SMEs' transitional capabilities towards digital technology. The corporation operates the LevelUP Accelerator programme, which assists selected SMEs in accessing digital markets and partnering with international e-commerce entities. JEDCO also provides technical training, consulting services, and financial support initiatives to facilitate SMEs' e-commerce exports.

○ For manufacturing SMEs, the Jordan Industry 4.0 & Digitalization Innovation Centre, established with European Union support, offers resources, facilities, and training programmes to advance innovation and digitalisation efforts. The centre aims to equip manufacturing SMEs with the tools and knowledge necessary for digital transformation.



○ Recent initiatives have focused on supporting women-led businesses in their digitalisation efforts. The International Labour Organization's Digitalize Your Business (DYB) for Female Entrepreneurs programme provides assistance to women implementing digitalisation projects in their businesses. Concurrently, the UN Women's Empowering Women Through Digital Skills programme offers digital skills training to foster women's entrepreneurship development.



SOURCES

- Jordan 2025 – A National Vision and Strategy
- Ministry of Digital Economy and Entrepreneurship: Jordan National Digital Transformation & Implementation Plan
- Jordan National E-Commerce Strategy
- REACH 2025 Vision and Action Plan
- Jordan Enterprise Development Corporation: Strategic Plan for 2022-2025
- Jordan Enterprise Development Corporation: The LevelUP Accelerator program
- Jordan Enterprise Development Corporation: Developing Jordanian SMEs E-Commerce Exports Through Virtual Market Places
- Jordan Industry 4.0 & Digitalization Innovation Centre (InJo4.0)
- International Labour Organization: Digitalize Your Business (DYB) for Female Entrepreneurs program in Jordan
- United Nations: UN Women Empowering Women Through Digital Skills

A man and a woman are sitting at a wooden desk, looking at a laptop. The man, on the left, has a beard and is wearing a grey sweater and glasses. The woman, on the right, is wearing a thick orange knit sweater and glasses, and she is smiling. A warm, yellow lamp hangs above them. In the background, there are horizontal wooden slats and a window with blinds.

02

Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Jordan's digital economy across four key dimensions: digital economy size and activities, digital infrastructure and connectivity, digital skills, and digital government.



Size and Activities of the Digital Economy

To describe the size and activities of Jordan's digital economy, we used data provided by the World Trade Organization and conducted our own calculations. We specifically analyzed the share of advanced technology products in total trade, cross-border trade in telecommunications, computer, information and audiovisual services, and total digitally delivered services.

Advanced technology products accounted for 13.83% of Jordan's imports. The share of advanced technology products in exports was lower at 5.44%, indicating a technology trade imbalance

Figure 1:
Telecommunications, Computer, Information and Audiovisual Services

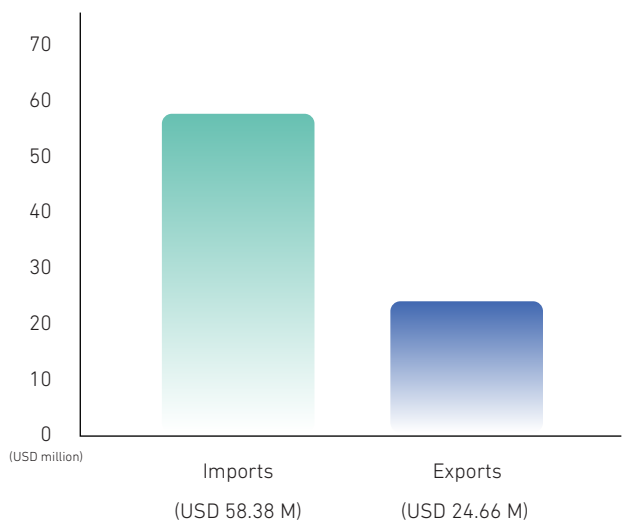


Figure 1 provides data for Jorden's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2:
Digital Delivered Services

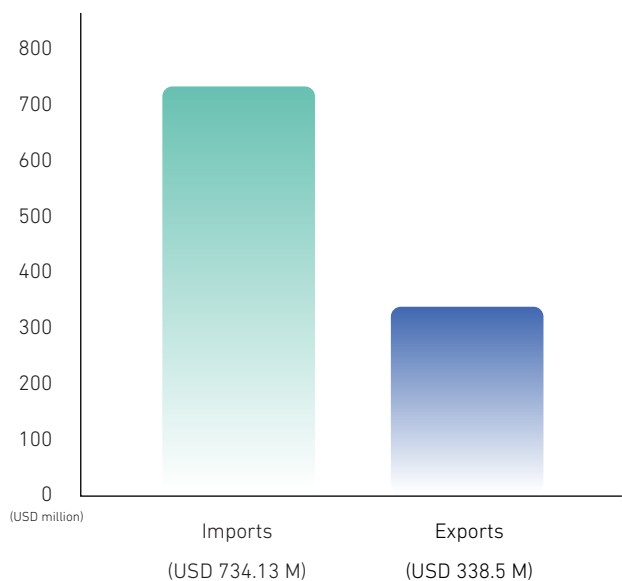


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Jordan's digital infrastructure and connectivity, we analyzed data provided by the International Telecommunications Union. We focused on internet access, broadband coverage, and traffic, as well as mobile phone ownership.

Figure 3:
Digital Infrastructure and Connectivity

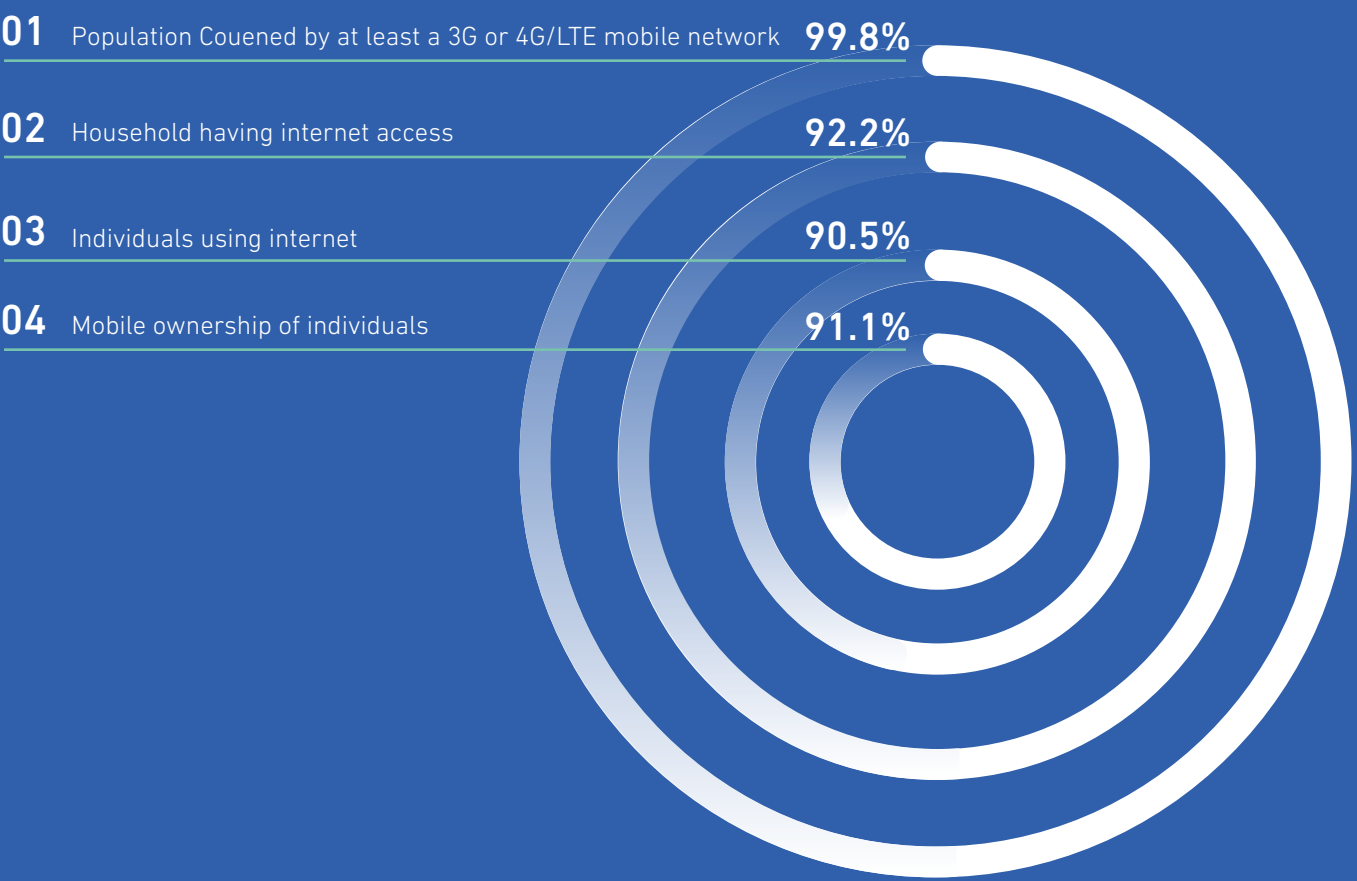
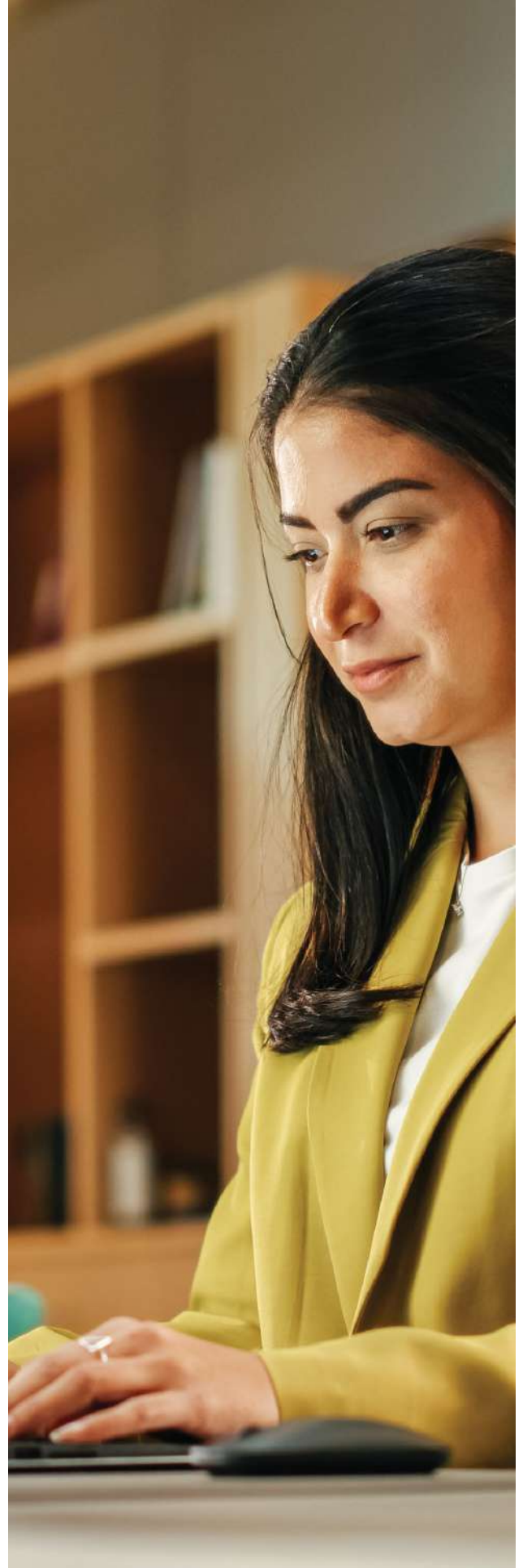


Figure 3 provides data to analyze Jordan's digital infrastructure and connectivity in 2022.

Digital Skills

To document Jordan's digital skills, we draw on data by UNESCO. We use data points relevant to general education, since no data points on specific digital skills (for instance on creating electronic presentations, copying files, or downloading software) were available in the UNESCO dataset for Jordan.

The upper secondary education completion rate in Jordan was **56.73%** in 2017. Gross tertiary education enrollment ratio stood at **33.06%** in 2023, indicating moderate participation in higher education. The adult literacy rate was **95%** in 2023. Government expenditure on education as a percentage of GDP was in 2021.





Digital Government

To examine the state of digital government in Jordan, we rely on the World Bank's GovTech dataset. Specifically, we analyze how Jordan provides digital government services, establishes institutions, and drafts strategies.

In terms of digital government services in 2022, Jordan had an operational government cloud platform in use. It had implemented a government interoperability framework. It had an advisory/R&D government open-source software policy. Jordan maintained both an open government portal and an open data portal. Regarding institutional frameworks for digital government in 2022, Jordan had established a government entity focused on government technology or digital transformation. It had established a government entity focused on public sector innovation. Jordan had institutionalized a whole-of-government approach to public sector digital transformation.

Finally, Jordan had drafted various strategies to advance digital government in 2022:

- 01 It had a current government technology or digital transformation strategy
- 02 It had both a strategy and program to improve digital skills in the public sector
- 03 It had both a strategy and program to improve public sector innovation



03

International Commitments and Collaboration

International Commitments and Collaboration

The purpose of this section is to outline the existing international commitments of Jordan and explain in which fora it engages in. We focus on international commitments and collaboration with a digital component, meaning a connection to the pertinent policy areas explained above.

To outline international commitments, we analyse binding free trade agreements and conventions, as well as non-binding guidelines/recommendations/principles and model laws. We also reference other commitments, both binding and non-binding. For each commitment, we explain whether it is binding and which policy area(s) it can impact. Regarding international fora, we analyse participation in discussions at the pluri- and multilateral level.





Commitments

Free Trade Agreements

Jordan has entered the following free trade agreements, which include provisions related to digital trade:

- 01 Jordan - United States Free Trade Agreement (Customs duties)
- 02 Jordan - Singapore Free Trade Agreement (Customs duties)
- 03 Jordan - Canada Free Trade Agreement (Customs duties)

Conventions

Jordan is party to the following conventions and agreements:

- 01 International Covenant on Civil and Political Rights (Data Protection)

- 02 G20/Organisation for Economic Co-operation and Development Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (Taxation)
- 03 League of Arab States Convention on Combating Information Technology Offences [Third-party source] (Cybersecurity)
- 04 Berne Convention for the Protection of Literary and Artistic Works (Source Code)

Guidelines, Recommendations, and Principles

Jordan is a member state of the United Nations, which has adopted the following frameworks:

- 01 United Nations Guidelines for Consumer Protection (Online Consumer Protection)

- 02 United Nations Educational, Scientific and Cultural Organization Recommendation on the Ethics of Artificial Intelligence (Artificial Intelligence)
- 03 United Nations draft Resolution A/78/L.49 on Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (Artificial Intelligence)

Jordan is a member state of the United Nations Economic and Social Commission for Western Asia (ESCWA), which has adopted the following frameworks:

- 01 ESCWA Guideline on e-communication and freedom of expression (Electronic transactions)
- 02 ESCWA Guideline on e-transactions and e-signatures (Electronic transactions)
- 03 ESCWA Guideline on e-commerce and consumer protection (Online consumer protection)
- 04 ESCWA Guideline on personal data protection (Data protection)
- 05 ESCWA Guideline on cybercrime (Cybersecurity)
- 06 ESCWA Guideline on intellectual property rights in cyberspace (Source Code)

Models

Jordan has adopted or been influenced by the United Nations Commission on International Trade Law Model Law on Electronic Commerce. (Electronic Transactions)



Other Commitments

- Jordan is a member of the World Trade Organization and as such is subject to the Moratorium on Customs Duties on Electronic Transmissions (Customs Duties), the Trade Facilitation Agreement (Trade Facilitation) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (Source Code).
- Jordan has implemented the United Nations Conference on Trade and Development Automated System for Customs Data. (Trade Facilitation with Digital Means)

Jordan is a member of the International Organization for Standardization, which has issued various technical standards including:

- ISO/IEC 22989:2022 (Information technology — Artificial intelligence — Artificial intelligence concepts and terminology) (Artificial Intelligence)

- ISO/IEC 42001:2023 (Information technology — Artificial intelligence — Management system) (Artificial Intelligence)
- ISO 22376:2023 (Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal data format for authentication, verification and acquisition of data carried by a document or object) (Cybersecurity)
- ISO 31700-1:2023 (Consumer protection — Privacy by design for consumer goods and services) (Consumer protection)
- ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity)
- ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)
- ISO 23195:2021 (Security objectives of information systems of third-party payment services) (Electronic payments)
- ISO 32111:2023 (Transaction assurance in E-commerce — Principles and framework) (Electronic transactions)

Fora

Jordan participates in the following international fora that touch upon digital issues:

- United Nations Global Digital Compact (Cross-cutting)
- Arab Federation for Digital Economy (Cross-cutting)
- Arab Federation for Digital Economy Memorandum of Understanding to establish a new regional data centre in the Kingdom of Bahrain (Cross-cutting)
- Buna Payment System (Electronic payments)

