Digital Cooperation Organization

Oman

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.

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

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:
Express consent is required for data processing, as well as transparency, honesty, and respect for human dignity. Data subjects have the rights to information, access, deletion, and portability. Authorisation is required to process sensitive personal data, as well as the appointment of data protection officers and external auditor, and registration, in specific scenarios.

Cross-Border Data Transfers:
Data transfers require the express consent of the data subject. Exceptions are foreseen for transfers that implement international agreements and for transfers that do not reveal the data subject's identity.

Location of Computing Facilities:
Oman does not generally require data to be localised. Local storage is required regarding classified government data, including by private entities. Further localisation mandates apply to telecommunications and Internet of Things providers.

Online Consumer Protection:
Online consumers are protected under the general consumer protection framework. It prohibits practices, including misleading information. The sending of unsolicited messages (spam) is regulated from a data protection, consumer protection, and telecommunications perspective.

Electronic Transactions:
The validity of electronic transactions (as well as messages, records, and documents) is established. Electronic signatures have the same legal effect of wet-ink signatures, with certain conditions, without differentiating types thereof.

Trade Facilitation with Digital Means:

Oman provides trade administration documents in electronic form and enables electronic submission. The Customs Single Window (Bayan), a one-stop shop for trade declarations and procedures, is operational and designed for international interoperability.

Cybersecurity:

Cybersecurity obligations are based on the classification of data, including specific rules for "confidential data." Notification is required in view of data breaches, including information on measures taken against the breach.

Artificial Intelligence:

There is currently no specific binding framework on the governance of AI. The government has signalled its intention to develop the local AI sector in several policy documents, including the National Program for AI and Advanced Technologies and the Policy on AI systems use.

Source Code:

The copyright law protects computer programs and databases, granting economic rights, with exceptions. For computer programs, a contract is to regulate the transfer of the economic rights. Oman does not mandate source code sharing.

Digital Economy Taxation and Customs Duties:

Digital services and products are not subject to customs duties but are explicitly subject to value-added tax. E-commerce imports are subject to value-added-tax and customs duties. Oman does not impose specific direct taxes on providers of digital services/products.

Electronic Payments:

Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to digital providers. All payment providers are subject to a licensing requirement under the central bank.

SMEs and Digital Inclusion:

Oman has implemented a range of initiatives to support SMEs and disadvantaged groups in leveraging digital technologies for trade. These efforts encompass broad digitalisation strategies, e-commerce support, digital skills development, and targeted programmes for specific sectors and demographics.

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 MS'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

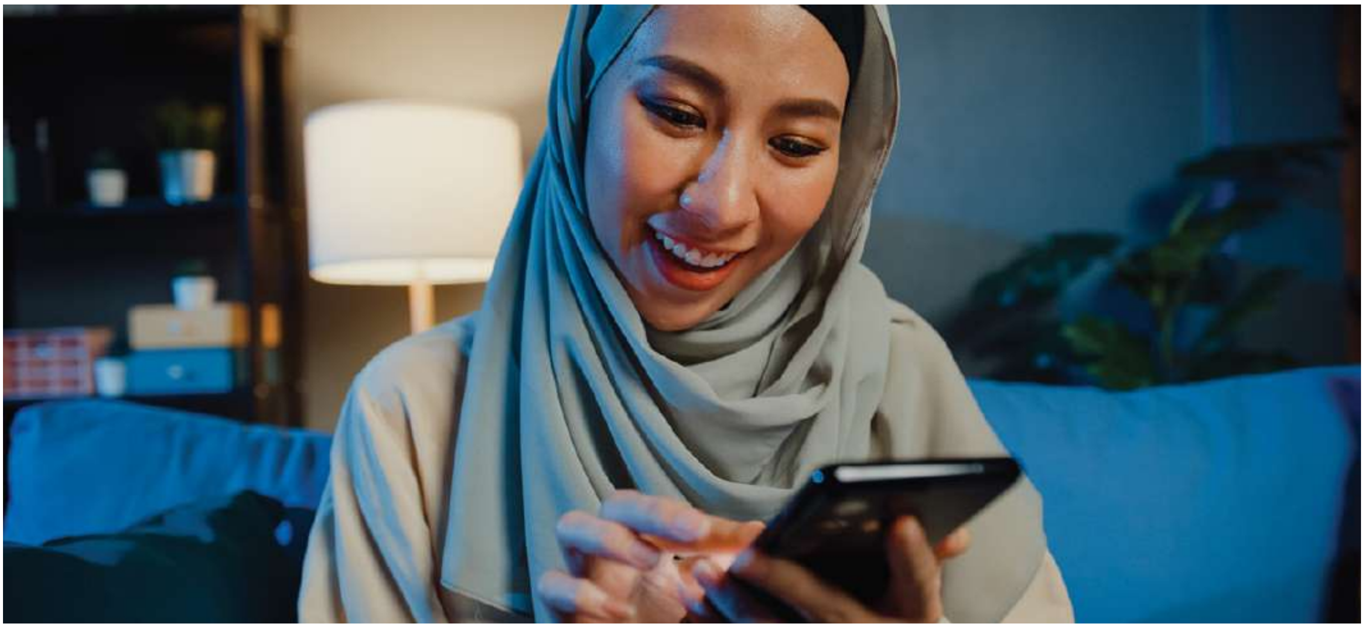
08 Artificial Intelligence

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.

Oman's data protection law requires express consent for data processing, as well as transparency, honesty, and respect for human dignity. Data subjects have the rights to information, to access, amend, request erasure, and transfer their data to other data controllers, as well as to revoke consent. Data controllers must get an authorisation before processing sensitive personal data. Data processors must appoint a personal data protection officer and an external auditor (upon request) and register with the government, if they meet certain conditions to be determined by regulation. The Ministry of Transport, Communications and Information Technology is responsible for oversight.

Summary

- The Personal Data Protection Law, in effect since 2023, regulates data processing. The law requires data to be processed with transparency, honesty, respect for human dignity, and only with the express consent of the personal data subject. The request for processing personal data must be in writing, clearly, explicitly and understandably. Data subjects are granted the rights to information, to access, amend, request erasure, and transfer their data to other data controllers, as well as to revoke content.

- The law further mandates approval from the Ministry of Transport, Communications and Information Technology for the processing of personal data related to genetics, health, sexual, and political data. Additionally, data controllers must appoint an external auditor to assess data protection measures.

- The Ministry of Transport, Communications and Information Technology issued the Executive Regulation for the Personal Data Protection Law in January 2024, including a one-year transitional period for full compliance. The regulation specifies provisions on personal data protection for children, data subject rights, data controllers' obligations, data breaches, cross-border data transfers, and penalties.

- The Ministry of Transport, Communications and Information Technology is responsible for overseeing personal data protection in Oman. The Ministry handles complaints, while the competent court issues penalties.

- The Regulation on Beneficiary Rights in Telecommunications Services establishes various obligations. Licensees must establish a policy for protecting the confidentiality and privacy of beneficiaries' personal data, approved by the authority, in the unified service agreement.

- Licensees can request the personal data of the beneficiary in accordance with the provisions of the Personal Data Protection Law, if the data is necessary to activate the required service, but must ensure the confidentiality and privacy of said data.

- The Regulation emphasises the protection of children, requiring licensees to establish a child protection policy, approved by the authority, that protects children who contribute content online through participation in programs, films, games, news, and more.

- This Regulation repeals a previous Regulation on Protection of the Confidentiality and Privacy of Beneficiary Data that required the written approval of the beneficiary so for telecommunications licensees to publish or exchange the data with subsidiaries or other companies.

- Finally, the Ministry issued the Personal Data Protection Policy in 2024, to be implemented by government agencies. It aims to benefit from the value of data and increase confidence in the government.

SOURCES

Primary Legislation

- Personal Data Protection Law No. 6 for the year 2022

Secondary Legislation

- Ministry of Transport, Communications and Information Technology: Executive Regulation No. 34 for the year 2024 for the Personal Data Protection Law
- Regulation on Beneficiary Rights in Telecommunications Services
- Telecommunications Regulatory Authority: Regulations on Protection of the Confidentiality and Privacy of Beneficiary Data [repealed]
- Personal Data Protection Policy, 2024

Oversight Authorities

- Ministry of Transport, Communication, and Information Technology

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 transfers are subject to specific conditions. Generally, transfers shall not prejudice national security and the transferor must assess and ensure that the recipient provides equivalent data protection. In addition, data transfers require the explicit consent of the data subject. Exceptions are foreseen for transfers that implement international agreements and for transfers that do not reveal the data subject’s identity. Moreover, government approval is required for the transfer of government data.

Summary

The Personal Data Protection Law establishes specific rules for cross-border data transfers. Cross-border data transfers are only allowed if they do not conflict with the operations of the Cyber Defence centre, do not violate the law, and do not potentially harm the data subject.

The Executive Regulation for the Personal Data Protection Law, approved in January 2024, includes a one-year transitional period for full compliance. The regulation mandates obtaining the data subject's consent before any cross-border data transfer, ensuring that such transfers do not compromise national security.

However, consent is not required if the transfer is part of implementing international commitments or does not reveal the data subject's identity. The data controller must ensure that the recipient of the data provides a level of protection at least equivalent to that in Oman.

Additionally, the controller is required to conduct an assessment of the recipient's data protection standards and the risks of the data transfer. The assessment must include a description of the nature and size of the data to be transferred, the degree of its sensitivity, the purpose and scope, the recipient, the time period and the regularity, and the final destination of the transfer.

The Personal Data Protection Policy states that controllers must process personal data within the geographical boundaries of Oman to preserve national sovereignty and the protection of privacy.

Data may not be transferred or processed abroad except in the execution of a contract to which the data subject is a party, the initiation of procedures for the claim or defense of legal rights, and the protection of the vital interests of the data subject. The controller must further obtain approval from the Cyber Defense Center before transferring personal data abroad.

Further data transfer conditions apply to government data. The Cloud First Policy establishes procedures for government agencies and private sector companies handling government data and wanting to store such data abroad. Storage abroad should be limited to Software as a Service and requires the approval of the Cyber Defense Center.

SOURCES

Secondary Legislation

- Personal Data Protection Law No. 6 for the year 2022

Secondary Legislation

- Ministry of Transport, Communications and Information Technology: Executive Regulation No. 34 for the year 2024 for the Personal Data Protection Law

Guidelines

- Personal Data Protection Policy, 2024
- Cloud Governance Framework
- Cloud First Policy

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.

Oman generally does not require data to be localised. Local storage requirements regulate government data storage, including by private entities that handle government data. Specifically, classified government data is to be stored locally, unless the competent authority issues a prior written approval. Further localisation mandates apply to telecommunications and Internet of Things providers.

Summary

- Oman generally does not require data to be localised but demands localisation for certain government data. Specifically, the Law on the Classification of State Records and the Governance of Protected Places states that classified documents shall be kept in designated places in government units and prohibits their transfer. Prior written approval from the competent authority is required to overcome the localisation requirement.

- The Regulation on Providing Internet of Things Services, issued by the Telecommunications Regulatory Authority, requires Internet of Things service providers to localise SMS, customer support centres, any equipment or devices used in storing customers data, as well as Internet of Things portals in Oman. It prohibits the transfer of such data outside Oman.

- For telecommunications, the Regulation on Beneficiary Rights in Telecommunications Services requires the systems and devices used to provide the service and store beneficiaries' data to be located in Oman.

- Furthermore, the Regulation Governing the Provision of Voice or Video Telecommunications Service over Internet Protocol imposes a data localisation requirement on voice or video telecommunication service providers, requiring data centres for the personal data of the beneficiary to be located and kept within the geographical boundaries of Oman.

- This includes the billing used for the service as well as the records for the calls, usage details, payment, and any recorded personal data of beneficiaries. The Telecommunications Regulatory Authority issued the Regulation for Data Centers and Cloud Computing with the aim of enhancing investment in data centers, improving the quality of data centers and cloud services, and establishing a regulatory basis for managing security risks.

- The regulation defines the key aspects and provisions related to providing data center and cloud computing services, the requirements for obtaining a permit to establish and operate data centers, and establishing and operating the infrastructure for the cloud computing system and providing related services.

- It also details the conditions and obligations for licensees to apply certain standards to achieve the highest levels of efficiency in operating data centers and clarifies the requirements for transferring data outside Oman.

  A chapter dedicated to information security classifies subscriber content into four levels and emphasises the importance of protecting subscriber data according to the best international standards.

SOURCES

Primary legislation

- Law on the Classification of State Records and the Governance of Protected Places

Secondary legislation

- Regulation on providing Internet of Things Services
- Regulation on Beneficiary Rights in Telecommunications Services
- Regulation for Data Centers and Cloud Computing
- Regulation Governing the Provision of Voice or Video Telecommunications Service over Internet Protocol [third party source]

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 in Oman are protected under the general consumer protection framework, primarily governed by the consumer protection law. The law prohibits certain practices, including providing misleading information, and requires providers to compensate consumers if they fail to deliver products or provide services. E-commerce platforms must obtain a licence, uphold transparency measures, and establish consumer complaint mechanisms. Spam is regulated from a data protection, consumer protection, and telecommunications perspective. The Consumer Protection Authority is responsible for oversight.

Summary

The Consumer Protection Law, enacted in 2014, includes provisions that address consumer rights, such as guarantee, returns, refunds, and compensations. It also delineates the obligations of providers, advertisers, and agents. Specifically, providers must obtain approval from the relevant authority for promotions, reduction of prices, and advertisements. Additionally, the Commercial Fraud Law, effective from 2021, provides additional consumer protection, including compensation for defective products.

The Consumer Protection Authority is responsible for the implementation of the Consumer Protection Law and the Commercial Fraud Law. The Authority issued the Executive Regulation implementing the Consumer Protection Law in 2017. It specifies provisions, consumer rights, and oversight procedures. In addition, the Central Bank of Oman issued the Financial Consumer Protection Regulatory Framework to enhance fairness in the financial sector.

The E-Commerce Regulation includes provisions related to consumer protection for e-commerce providers, who must obtain a licence from the Ministry of Commerce, Industry, and Investment Promotion. In addition, e-commerce providers must give correct information on goods and services, implement measures to protect consumers' personal data, establish procedures for receiving and handling consumer complaints, and be transparent regarding their exchange and return policy and their terms and conditions.

The Consumer Guide Electronic Application provides average prices for products and allows consumers to submit complaints. The Regulation on the Practice of Marketing and Promotion Activity on Websites and Social Media, which came into force in 2023, requires licensing for marketing and promotion providers. Exceptions are foreseen for non-profit entities and providers who have obtained another licence.

Spam is regulated from a data protection, consumer protection, and telecommunications perspective. The executive regulation of the data protection law requires that, before sending any advertising or marketing material with commercial purpose to the personal data subject, the controller must adhere to the following procedures: Obtain the written consent of the personal data subject; notify the personal data subject of the methods; specify the mechanism to opt-out; and immediately cease sending upon request from the personal data subject, free of charge.

The executive regulation of the consumer protection law requires that, before conducting promotions, providers must: Obtain the approval of the authority, after coordination to ensure that there are no misleading offers or advertisements, including ensuring that there are no misleading offers or advertisements, and providing a copy of the approval to the authority.

The Regulation on Beneficiary Rights in Telecommunications Services includes a chapter commercial or promotional messages and generally prohibits the sending of spam messages, via SMS, MMS, email, or other telecommunications services.

Sending such messages requires the recipient's prior consent, in a method specified by the licensee and approved by the authority. Previously, the Telecommunications Regulatory Authority published a Draft Resolution to Issue Anti-SPAM Regulations for consultation in 2012. The Resolution would have required explicit consent for spam.

Finally, the Ministry of Commerce, Industry and Investment Promotion has worked on developing a platform which provides a list of registered businesses, to allow consumers to verify legitimate platforms and increase confidence in e-commerce.

SOURCES

Primary Legislation

- Consumer Protection Law for the year 2014
- The law implementing the GCC commercial fraud law for the year 2021

Secondary Legislation

- Consumer Protection Authority: The Executive Regulations for the Consumer Protection Law
- Regulation on Beneficiary Rights in Telecommunications Services
- Ministry of Transport, Communications and Information Technology: Executive Regulation No. 34 for the year 2024 for the Personal Data Protection Law
- E-Commerce Implementing Regulation, 2023
- Central Bank of Oman: Financial consumer protection regulatory framework
- Regulation on the Practice of Marketing and Promotion Activity on Websites and Social Media, 2022
- Public Consultation on Draft Resolution to Issue Anti-SPAM Regulations

Guidelines

- Consumer Protection Authority: The Consumer Guide Electronic Application

Oversight Authorities

- The Consumer Protection Authority

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 in Oman are governed by several legal acts, mainly the electronic transactions law. The law recognises the validity of electronic transactions (as well as messages, records, and documents). The law further states that the electronic signatures have the same legal effect of wet-ink signatures, with certain conditions, but does not differentiate different types thereof. Regarding electronic authentication, the government licences authentication services and a national eID scheme.

Summary

- The Electronic Transactions Law, which came into force in 2008, grants electronic transactions, records, signatures, and messages the same legal effect as paper-based alternatives. Exceptions include matters related to personal status, such as marriage or wills, and court procedures, as well as any document that must be notarised.

- The Law aims at facilitating electronic transactions by using reliable electronic messages or records, and removing any obstacles or challenges encountering electronic transactions. To this end, it establishes criteria for electronic messages to carry evidential weight.

- The law further establishes criteria under which electronic signatures have the same legal effect of real signatures, including impeding post-signature changes Electronic signatures are authenticated by bodies defined in the Law. The Ministry of Transport, Communications, and Information Technology oversees the implementation of the Electronic Transactions Law.

- The National Digital Certification Center provides online digital certification ("TAM") through the ID/Resident Card and SIM Card. It enables the users to complete transactions online without the need of having to be physically present at service providers' locations. The Digital ID is activated by the Royal Oman Police. The Oman National Computer Emergency Readiness Team provides electronic authentication services through its portal for individuals, public agencies, and private sector companies.

- The Ministry of Commerce, Industry and Investment Promotion issued the National E-Commerce Plan, covering eight pillars. Under this plan, 30 initiatives across 13 entities were rolled out, reaching 70% completion, and a High-level Committee for E-commerce was established to oversee the implementation. Previously, the Ministry of Commerce, Industry and Investment Promotion issued a regulation on e-commerce regulation that is not yet public.

SOURCES

Primary Legislation

- Electronic Transactions Law for the year 2008

Guidelines

- National E-Commerce Plan in the Sultanate of Oman [source not working]
- Electronic Authentication Services
- Digital IDs
- User Guide for Digital Certification Service "TAM"

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.

Oman provides trade administration documents in electronic form and enables electronic submission. The Customs Single Window (Bayan), designed as a one-stop shop for trade declarations and procedures, is operational. Bayan is designed for international interoperability. There are no publicly available online sources regarding expedited customs procedures for low-value shipments.

Summary

- Oman's paperless trade system is supported by several key legislative frameworks and technological advancements. The Electronic Transactions Law provides the legal foundation for the use of electronic records and signatures, ensuring the validity of digital transactions.

- The Bayan single window integrates three key systems: an Integrated Customs Management System for all customs operations, an Electronic Single Window for trade-related matters and a Risk Management System that categorises shipments for inspection and clearance. The system allows electronic submission of import and export documents and applying for required licences, permits, and exemptions.

- Since its launch in 2015, Bayan has simplified trade by enabling the electronic submission of customs documents, prior clearance, and reducing processing times. It includes 35 sub-systems to facilitate permit approvals within 24 hours and conducts a "one-stop inspection" within two hours. The system supports international data exchange and has expedited procedures for low-value shipments, improving data exchange. Furthermore, the Oman business platform facilitates the establishment of a new business in Oman, including licensing.

- The Ministry of Commerce, Industry and Investment Promotion developed the National Action Plan which aims to transform Oman into a regional e-commerce hub and build a thriving e-commerce sector by 2027. The action plan includes transport, logistics, and trade facilitation among its enabling pillars and several initiatives including fair and transparent customs duties on e-commerce shipments.

SOURCES

Primary Legislation

- Electronic Transactions Law for the year 2008

Guidelines

- The Customs Single Window (Bayan)
- National Action Plan in the Sultanate in Oman
- Customs Exemptions

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.

Cybersecurity is regulated by the cybercrime law and other laws, including the data protection law. Obligations are based on the classification and thus risk level of data, including specific rules for "confidential data." The data protection law requires incident notification for breaches and privacy violations, including information on measures taken against the breach. The Ministry of Transport, Communications, and Information Technology, is in charge of oversight.

Summary

- The Cyber Crime Law, in effect since 2011, governs all information technology crimes impacting Oman's interests, even if they occur or are planned outside the country. The law defines various cyber-related offences, including unauthorised access to databases and websites with the intent to alter, delete, copy, or publish data, as well as actions aimed at destroying data systems and networks. The law outlines penalties for these offences, with harsher consequences if the data involved is personal or pertains to government information. In addition, the data protection law requires incident notification for data breaches, including information on mitigation measures.

- The main regulatory authority for cybersecurity in Oman is the Cyber Defense Center, which aims to enhance the ability of concerned entities and individuals to counter electronic threats and to build national capabilities specialized in cybersecurity by creating partnerships between relevant sectors locally and internationally.

- The Ministry of Transport, Communications and Information Technology (MTCIT, previously the Information Technology Authority) also oversees cybersecurity initiatives, policies, frameworks, and guidelines. The Oman National Computer Emergency Readiness Team (OCERT) operates under the MTCIT and focuses on incident response, cybersecurity awareness, and coordination among various stakeholders. Penalties are determined by courts.

- The MTCIT recently issued the Cybersecurity Industry Development Program, to advance cybersecurity as an economic sector. In addition, the Cybersecurity Governance Guidelines which aims to enable a uniform governance, risk management and security management framework for government agencies. Finally, the Basic Security Controls establishes security baselines for government organisations in Oman to safeguard the valuable information assets within the organisation.

- The OCERT manages the Hadatha Program for Cybersecurity, which supports the development and enhancement of cybersecurity capabilities and the National Cybersecurity Index program, designed to improve Oman's cyber readiness and its ranking on the global cybersecurity index.

SOURCES

Primary Legislation

- Royal Decree No 12/2011, Cyber Crime Law of 2011
- Personal Data Protection Law No. 6 for the year 2022
- Royal Decree Establishing the Ministry of Transport, Communications and Information Technology, 2019

Guidelines

- Ministry of Transport, Communications and Information Technology: Cyber Security Industry Development Program
- Ministry of Transport, Communications and Information Technology: Cybersecurity Governance Guidelines
- Ministry of Transport, Communications and Information Technology: Basic Security Controls
- Oman National Computer Emergency Readiness Team: Hadatha Program for Cyber Security
- Oman National Computer Emergency Readiness Team: National Cybersecurity Index program

Oversight Authorities

- Oman National Computer Emergency Readiness Team (OCERT)
- Ministry of Transport, Communications and Information Technology

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 binding framework on the governance of AI. As such, there are no risk-based nor technology-specific requirements that apply to AI providers. The government has signalled its intention to develop the local AI sector and enhance government use of AI in several policy documents, including the National Program for AI and Advanced Technologies, which updates and expands the Executive Program for AI and Advanced Technologies, and the Policy on AI systems use. No regulatory agencies have issued guidelines on how existing rules apply to AI providers.

Summary

- There is currently no AI-specific primary or secondary legislation in Oman. The Ministry of Transport, Communication and Information Technology developed the Executive Program on AI and advanced technologies in 2020. It strives for Oman to be in the top 35 countries in the Governmental Readiness Index for AI by 2030, by increasing the number of AI startups by 20% annually, increasing investments to reach USD 400 million in 2030, and increasing the number of research papers by 20% annually.

- Given the rapid developments of AI and advanced technologies, in 2024, the executive program was adapted to become a comprehensive national program. It takes into account economic and social aspects, in line with the global developments in the field of AI, especially in light of the emergence of generative AI technologies.

- This upgrade aims to enhance the utilization of AI applications and cater for the economic and development sectors. The national program also includes a set of specialized programs and initiatives in the field of AI, in line with national directions as well as Oman's Vision 2040.

  The Ministry also developed the Policy on AI systems use, which aims to enable government agencies to make use of AI systems and enhance the use of AI in different economic sectors, as well as a document on Future Opportunities in AI and Advanced Technologies in Oman.

- The National Centre for Space, AI and Advanced Technologies under the Ministry of Transport, Communication and Information Technology was established in 2020. One of its main tasks is to implement the Executive Program on AI and Advanced Technologies. The centre reports to the Financial and Economic Committee emanating from the Council of Ministers.

SOURCES

Guidelines

- National Program on AI and advanced technologies
- Executive Program on AI and advanced technologies
- Policy on AI Systems Use [third party source]
- Future opportunities in AI and Advanced Technologies

Oversight Authorities

- The National Centre for Space, AI and Advanced Technologies
- Ministry of Transport, Communication and Information Technology

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.

Oman's copyright law protects computer programs and databases as works of literature, arts, and science. Protection provides authors with economic rights but foresees exceptions that allow the single reproduction of computer programs, for example for backup purposes. In addition, for computer programs, a contract is to regulate the transfer of the economic rights. Oman does not mandate source code sharing.

Summary

- The Copyright Law protects computer programs and databases as works of literature, arts, and science, whether readable from the computer or other. The protection grants economic rights, including the right to compensation and to transfer the rights.

- The transfer of economic rights, in respect to the works of computer programs and applications or databases, shall be subject to authorisation of the contract attached to the program.

- The Industrial Property Rights Law regulates the conditions and procedures for obtaining patents, including computer program code. It provides exceptions for industrial processes consisting of steps performed by a computer and for products composed of elements of an invention executed by a computer, including computer-readable program codes stored on a tangible medium and general-purpose computers.

  The Law foresees cases in which the use of computer programs is lawful even without the consent of the author, including the reproduction or adaptation of a single copy of a computer program by the lawful owner of the copy, if it is necessary for the use of the computer program or for archival purposes, or to replace the lawfully owned copy of the computer program in the event that the original copy is lost, destroyed or rendered unusable.

SOURCES

Primary Legislation

- Industrial Property Rights Law
- Law of Copyrights and Neighbouring Right
- Implementing Regulation of the GCC Common Customs Law
- Minimum VAT registration Decision No.1, 2021

Guidelines

- VAT Registration Application for Non-Residents
- VAT Guideline (Electronic Commerce)

Oversight Authorities

- Oman Tax Authority
- Directorate General of Customs

Digital Economy Taxation and Customs Duties

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.

Digital services and products are not subject to customs duties but are explicitly subject to value-added-tax. E-commerce imports are subject to value-added-tax and customs duties. Tax registration is required for non-resident entities (and for local entities whose yearly sales exceed OMD 38,500). Oman does not impose specific direct taxes on providers of digital services or digital products. The Oman Tax Authority enables electronic tax registration for non-residents.

Summary

- Customs duties do not apply to digital services/products but they do apply to e-commerce imports. There is no de minimis threshold exempting low-value e-commerce imports.

  Oman is an active member of the Gulf Cooperation Council (GCC) and the GCC Customs Union. The Unified Customs Law of the GCC States aligns Oman's customs procedures with those of other GCC member states, although it is not yet fully implemented.

- The Value Added Tax (VAT) Law applies to electronically supplied services, establishing that VAT is due if the place of actual use or benefit of such services is Oman. The VAT, set at a rate of 5% in line with the Gulf Cooperation Council, is elaborated in the VAT Regulation. Non-resident providers must register for the VAT, with no threshold, while resident companies must only if their yearly sales exceed OMR 38,500.

- Non-resident service providers can register by filling VAT registration applications and sending it to the tax authority by email, along with the required documents. They are further required to appoint a tax representative in Oman.

  Oman does not impose specific direct taxes on providers of digital services or digital products.

SOURCES

Primary Legislation

- \- Value Added Tax Law
- \- GCC Common Customs Law

Secondary Legislation

- \- Value Added Tax Regulation

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 in Oman are governed by the general regulatory framework for payments. Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules, enshrined in the Law on Combating Money Laundering and Terrorism Financing, apply to digital providers, too. Specifically, customer due diligence is required before establishing business relationships or before carrying out transactions of over OMR 6000, when the business relationship is not yet established. All payment providers are subject to a licensing requirement under the central bank.

Summary

- The National Payment Systems Law and its Implementing Regulations, overseen by the Central Bank of Oman, cover all payment kinds and systems, including electronic money. The Law requires any company to be licensed by the bank to provide payment services and the Implementing Regulation specifies the licensing process and requirements.

  The Law regulates electronic money specifically, which is accepted as a means of payment and differentiated from digital and virtual currencies. Issuing electronic money is not allowed without obtaining a licence from the central bank.

- The Law on Combating Money Laundering and Terrorism Financing establishes customer due diligence and risk management measures for financial institutions, among others. The Instructions for all Financial Institutions specify circumstances in which financial institutions are to undertake customer due diligence in the following circumstances.

- Namely, before establishing a business relationship or before carrying out a transaction for a customer with whom no established business relationship exists, if the value of the transaction exceeds OMR 6000.

- The Ministry of Commerce, Industry and Investment Promotion also published a ministerial decision regarding electronic payment services. It plans to expand to other sectors, including electronic shops, and to collaborate with the Central Bank to reduce frictions in electronic payments.

- The Central Bank of Oman operates an e-payment system, internally, for prepaid and debit cards. It is not in charge of credit cards and of international matters, for which there is a separate system (through banks directly).

SOURCES

Primary Legislation

- National Payment Systems Law, 2018
- Law on Combating Money Laundering and Terrorism Financing No. 30, 2016

Secondary Legislation

- Implementing Regulation for the National Payment Systems Law, 2019
- Instructions for all Licensed Financial Institutions under the Supervision of Central Bank Of Oman on implementing Combating Money Laundering and Terrorism Financing Law (30/2016)
- Ministry of Commerce, Industry and Investment Promotion: Ministerial Decision 386/2022 regarding the Provision of the Electronic Payment Service to Consumers

Guidelines

- Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines for Financial Institutions
- Transaction Monitoring and Suspicious Transaction Reporting Guidelines [source not working]

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.

Oman has implemented a range of initiatives to support SMEs and disadvantaged groups in leveraging digital technologies for trade. These efforts encompass broad digitalisation strategies, e-commerce support, digital skills development, and targeted programmes for specific sectors and demographics. The initiatives are primarily driven by government entities and public-private partnerships, focusing on improving digital literacy, facilitating access to e-commerce platforms, and enhancing technical capabilities.

Summary

- The Sultanate of Oman's 'SME Digitalisation Drive', announced in 2019, aims to achieve an SME digitalisation rate of at least 80% by 2025. This initiative forms part of the broader National Program for Digital Economy, launched in 2020 under the Oman Vision 2040 framework. Whilst not exclusively targeting SMEs, this programme includes financial support schemes and skills development opportunities that benefit smaller enterprises.

- The Ministry of Commerce's National E-Commerce Plan provides specific support for SMEs through technical platforms, practical workshops, and business guidance. In 2022, the e-commerce platform Kushk was established with support from the Small and Medium Enterprises Development Authority (SMEDA), offering SMEs facilitated access and assistance in establishing an online presence.

- Digital skills development features prominently in Oman's SME support strategy. The Oman Small and Medium Enterprises Development Authority (SMEDA) operates the Riyada Academy, an online training platform for SME owners offering e-commerce and related courses. SMEDA also manages Eacademy, which aims to improve SMEs' digital competencies among other objectives.

- Sector-specific initiatives include the Rifi programme under the Ministry of Agriculture, Fisheries and Water Resources. This programme provides skills training to women in agriculture, with workshops focusing on digital marketing and after-sales services.

- In 2022, a Memorandum of Understanding between Microsoft and the Ministry of Transport, Communication and Information Technology was signed. Under this agreement, Microsoft will launch several initiatives to improve SMEs' digital skills, including in the field of Artificial Intelligence.

SOURCES

- Oman Vision 2040
- SME Digitalisation Drive [Press Report]
- The National Program for Digital Economy
- Ministry of Commerce, Industry and Investment Promotion: National E-Commerce Plan in the Sultanate of Oman
- Small and Medium Enterprises Development Authority: Access to Kushk
- Kushk
- Small and Medium Enterprises Development Authority: Riyada Academy
- Small and Medium Enterprises Development Authority: Eacademy
- Ministry of Agriculture, Fisheries and Water Resource: 'Rifi' empowers rural women for self-employed [Press Report]
- Microsoft: Microsoft to help MTCIT boost Digital Transformation efforts

02
Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Oman'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 Oman'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 9.18% of Oman's imports. The share of advanced technology products in exports was considerably lower at 0.95%, indicating a technology trade imbalance.

Figure 1: Telecommunications, Computer, Information and Audiovisual Services.

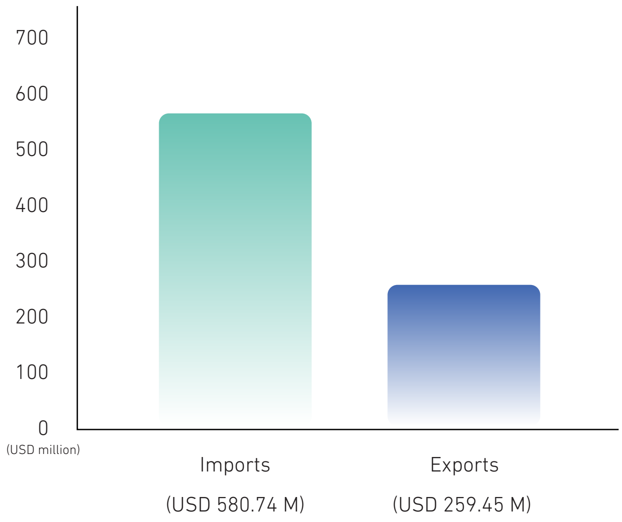


Figure 1 provides data for Oman's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

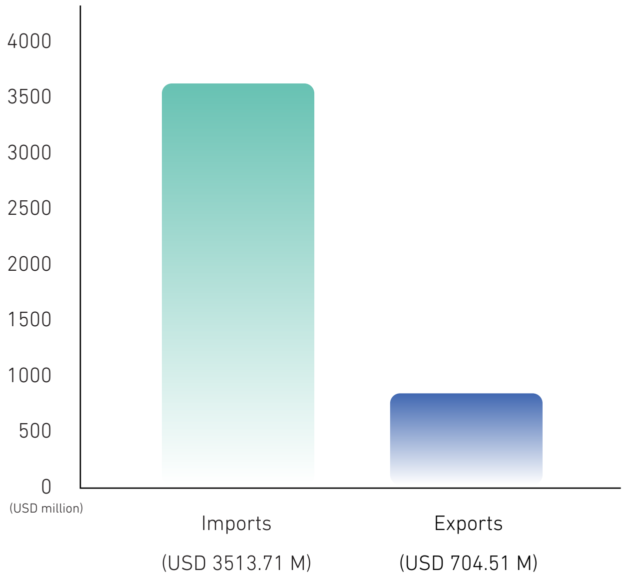


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Oman'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

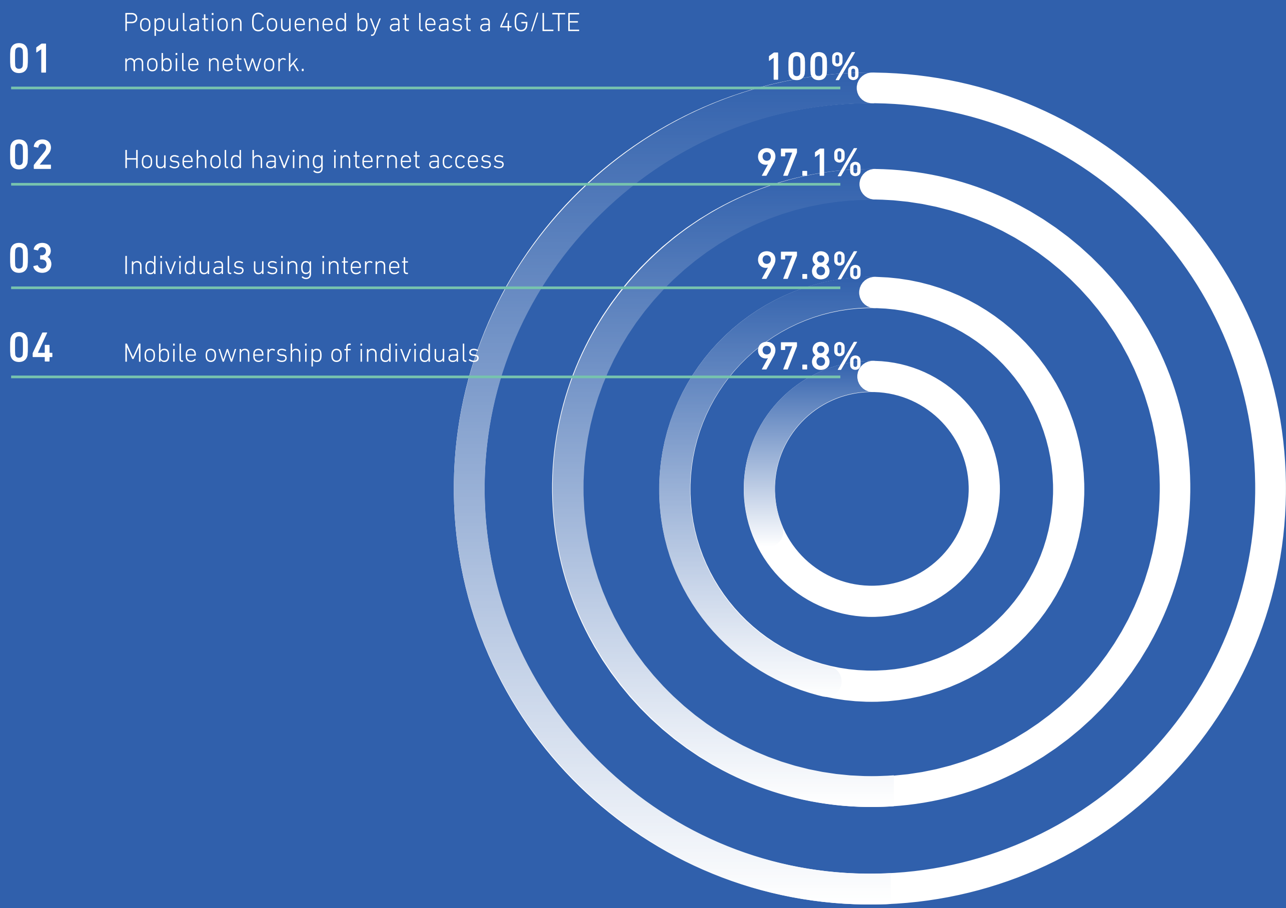


Figure 3 provides data to analyze Oman's digital infrastructure and connectivity in 2022.

Digital Skills

To document Oman's digital skills, we draw on data by UNESCO. We use data points relevant to digital skills, beginning with general education and moving to specific digital skills.

Gross tertiary education enrollment ratio stood at 45.59% in 2023, indicating moderate participation in higher education. The adult literacy rate was 97% in 2022. Government expenditure on education as a percentage of GDP was 0.35% in 2022.

The proportion of youth and adults with basic digital skills varied: In 2022, 23.74% had created electronic presentations with presentation software, whereas 66.91% found, downloaded, installed and configured software.

Digital Government

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

In terms of digital government services in 2022, Oman 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. Oman maintained both an open government portal and an open data portal.

Regarding institutional frameworks for digital government in 2022, Oman had established a government entity focused on government technology or digital transformation. It had established a government entity focused on public sector innovation. Oman had institutionalized a whole-of-government approach to public sector digital transformation.

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

01 It had a government technology or digital transformation strategy that needed to be updated

02 It had either a strategy or 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 Oman 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

Oman is part of the Free Trade Agreement signed between the Gulf Cooperation Council (GCC) and the European Free Trade Association (EFTA) States. This agreement includes an Annex on the exchange of information in the area of electronic commerce.

Oman has entered the Oman - United States Free Trade Agreement which contains provisions pertinent to Electronic Transactions, Online Consumer Protection and Customs Duties.

Conventions

Oman is party to the following conventions and agreements:

01 G20/Organisation for Economic Co-operation and Development Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (Taxation)

02 League of Arab States Convention on Combating Information Technology Offences [Third-party source] (Cybersecurity)

03 Gulf Cooperation Council Unified VAT Agreement (Taxation)

04 Gulf Cooperation Council Unified Economic Agreement (Cross-cutting)

05 Gulf Cooperation Council Common Customs Law (Customs Duties)

06 Gulf Cooperation Council Agreement of the Linking System for Payment Systems (Electronic Payments)

07 Berne Convention for the Protection of Literary and Artistic Works (Source Code)

Guidelines, Recommendations, and Principles

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

04 ESCWA Guideline on e-communication and freedom of expression (Electronic transactions)

05 ESCWA Guideline on e-transactions and e-signatures (Electronic transactions)

06 ESCWA Guideline on e-commerce and consumer protection (Online consumer protection)

07 ESCWA Guideline on personal data protection (Data protection)

08 ESCWA Guideline on cybercrime (Cybersecurity)

09 ESCWA Guideline on intellectual property rights in cyberspace (Source Code)

Models

01 Oman has adopted or been influenced by the following model frameworks:

02 United Nations Commission on International Trade Law Model Law on Electronic Commerce (Electronic Transactions)

03 United Nations Commission on International Trade Law Model Law on Electronic Signatures (Electronic Transactions)

Other Commitments

01 Oman 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). In addition, Oman is a participant in the Joint Statement Initiative which has finalised a stabilised text on the Agreement on Electronic Commerce on 26 July 2024.

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

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

04 ISO/IEC 42001:2023 (Information technology — Artificial intelligence — Management system) (Artificial Intelligence)

05 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)

06 ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity)

07 ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)

08 ISO 23195:2021 (Security objectives of information systems of third-party payment services) (Electronic payments)

09 ISO 32111:2023 (Transaction assurance in E-commerce — Principles and framework) (Electronic transactions)

Fora

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

02 United Nations Global Digital Compact (Cross-cutting)

03 Arab Federation for Digital Economy (Cross-cutting)

04 Arab Federation for Digital Economy Memorandum of Understanding to establish a new regional data centre in the Kingdom of Bahrain (Cross-cutting)

05 Arabian Gulf System for Financial Automated Quick Payment Transfers (Electronic payments)

06 Buna Payment System (Electronic payments)

Digital Cooperation Organization

@dcorg | www.dco.org