Digital Cooperation Organization

Qatar

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

01 Domestic Regulatory Environment Assessment 6

Data Protection 8
Cross-Border Data Transfers 13
Location of Computing Facilities 16
Online Consumer Protection 19
Electronic Transactions 23
Trade Facilitation with Digital Means 27
Cybersecurity 31
Artificial Intelligence 35
Source Code 39
Digital Economy Taxation and Customs Duties 42
Electronic Payments 46
SMEs and Digital Inclusion 50

02 Digital Economy Factsheet 48

Size and Activities of the Digital Economy 49
Digital Infrastructure and Connectivity 50
Digital Skills 51
Digital Government 52

03 International Commitments and Collaboration 53

Commitments 54
Fora 57

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:
Consent is required for data processing, with exceptions. Data subjects have the rights to information, access, rectification, and deletion, as well as to withdraw consent. There is no obligation to appoint a local representative or data protection officer, or to register.

Cross-Border Data Transfers:
Qatar emphasises the free flow of personal data. Data controllers are not allowed to restrict cross-border data flows, unless such processing contravenes the provisions of the law or causes significant harm to the data subject. Location of Computing Facilities: Qatar does not demand general data localisation, but maintains localisation requirements for government data and in the financial sector.

Online Consumer Protection:
Online consumers are protected by several laws which prohibit misrepresentations and charging consumers without authorisation, among others. The sending of unsolicited messages (spam) is generally forbidden without (express or inferred) consent and must include the contact details of the sender as well as an unsubscribe option.

Electronic Transactions:
The validity and enforceability of electronic communications to conduct transactions is established, with exceptions. Electronic signatures are recognised as valid, without differentiating types thereof.

Trade Facilitation with Digital Means:
Qatar provides trade administration documents for imports in electronic form and accepts electronic submissions. The Electronic Customs Clearance Single Window is operational and supports international document exchange.

Cybersecurity:

Qatar imposes security and risk assessment obligations based on its data classification. Cybersecurity incidents must be reported to authorities.

Penalties for cybercrimes are based on Artificial Intelligence:

Qatar does not have a specific regulatory framework for AI but is currently developing AI guardrails. The government has issued a national AI strategy and guidelines for the secure adoption and usage of AI.

Source Code:

The copyright law provides protection for computer programs, granting authors the exclusive rights, with exceptions. Source code sharing is not generally mandated although sectoral regulations in insurance and banking require providers to review the source code of "critical applications" to identify vulnerabilities.

Digital Economy Taxation and Customs Duties:

For digital services/products, Qatar imposes neither customs duties nor indirect taxes, although it is laying the foundation for a value-added-tax of 5%. For e-commerce imports, Qatar applies customs duties, but no indirect taxes. Qatar does not have a specific direct tax targeting providers of digital services/products.

Electronic Payments:

Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payment providers. No financial services can be delivered without a licence from the central bank.

SMEs and Digital Inclusion:

Qatar has implemented a range of initiatives to support SMEs and disadvantaged groups in accessing digital trade opportunities. These efforts, guided by the Qatar National Vision 2030 and the subsequent Digital Agenda 2030, encompass various programmes offering technical assistance, financial support, and digital infrastructure development.

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.

Qatar's privacy law generally requires consent for data processing but foresees exceptions, including the "lawful purpose" of the controller or public interest, among others.

Data subjects have the rights to information, access, rectification, and deletion, as well as to withdraw consent. There is no obligation to appoint a local representative or data protection officer, or to register with the government.

The National Cyber Security Agency, which reports directly to the Council of Ministers, is responsible for oversight.

Summary

- The Law on Protecting Personal Data Privacy, in effect since 2017, aims to ensure the protection of individuals' fundamental rights, particularly their right to privacy and data protection. The law applies to all processing of personal data by any organisation, including the private sector.

- The law requires organisations to process personal data with transparency, honesty, and respect of human dignity. Personal data with "special nature" (for example concerning ethnic origin, children, health, and criminal offences, among others) can only be processed after obtaining permission from authorities.

  The National Cyber Security Agency (NCSA), specifically the National Cyber Governance and Assurance Affairs division, is responsible for managing personal data protection matters in Qatar. It reports directly to the Council of Ministers.

- The NCSA can start investigations, impose fines, draft rules, provide guidance, and monitor compliance. Other authorities include the Communications Regulatory Authority for the telecommunications sector, and the Qatar Central Bank for banking and financial institutions.

  The NCSA has issued a guidance booklet on the Law on Protecting Personal Data Privacy, as well as guidelines for specific actors (controller and processor), and specific topics (data privacy impact assessment).

- In the Qatar Financial Centre, the Data Protection Office oversees data protection. The DPO is an independent institution and can initiate investigations, impose fines, draft, provide guidance, and monitor compliance.

  The Qatar Financial Centre establishes distinct data protection rules, namely the Data Protection Regulations and the Data Protection Rules. The DPO published guidance on these regulations and rules.

SOURCES

Primary Legislation

- Law No. 13 of 2016 on Protecting Personal Data Privacy

Secondary Legislation

- Amiri Decree No. 1 of 2021 establishing the National Cybersecurity Agency
- Qatar Financial Centre: Data Protection Regulations
- Qatar Financial Centre: Data Protection Rules
- Qatar Financial Centre: Data Protection Office: Oversight and Regulatory Action Framework
- Qatar Financial Centre: Data Protection Office: Supervisory Priorities
- Qatar Financial Centre Data Protection Office: List of Adequate Jurisdictions
- Qatar Financial Centre: Standard Contractual Clauses relating to the transfer of Personal Data outside the QFC pursuant to the QFC Data Protection Regulations 2021 ("QFC DPR 2021")
- Qatar Central Bank: Cloud Computing Regulation - Regulating the use of Cloud Computing by QCB-Licensed Entities

Guidelines

- National Cyber Security Agency: Personal Data Privacy Protection Law Overview
- National Cyber Security Agency: Controller and Processor - Guideline for Regulated Entities
- National Cyber Security Agency: Data Privacy Impact Assessment (DPIA) - Guideline for Regulated Entities
- National Cyber Security Agency: Data Privacy by Design and by Default - Guideline for Regulated Entities
- National Cyber Security Agency: Electronic Communications for Direct Marketing - Guideline for Regulated Entities
- National Cyber Security Agency: Exemptions Applicable to Competent Authorities (under Article 18) - Guideline for Regulated Entities
- National Cyber Security Agency: Exemptions Applicable to Data Controllers (under Article 19) - Guideline for Regulated Entities
- National Cyber Security Agency: Individuals' Complaints - Guideline for Regulated Entities
- National Cyber Security Agency: Individuals' Rights - Guideline for Regulated Entities
- National Cyber Security Agency: Personal Data Breach Notifications - Guideline for Regulated Entities
- National Cyber Security Agency: Principles of Data Privacy - Guideline for Regulated Entities
- National Cyber Security Agency: Privacy Notice - Guideline for Regulated Entities
- National Cyber Security Agency: Record of Processing Activities - Guideline for Regulated Entities
- National Cyber Security Agency: Special Nature Processing - Guideline for Regulated Entities
- National Cyber Security Agency: Individuals' Complaints - Guideline for Individuals
- National Cyber Security Agency: Individuals' Rights - Guideline for Individuals
- National Cyber Security Agency: Social Media - Guideline for individuals
- Qatar Financial Centre Data Protection Office: Data Protection Regulations & Rules 2021 Guidance
- Qatar Financial Centre Data Protection Office: Data Protection Regulations 2021 - Factsheet
- Qatar Financial Centre Data Protection Office: Data Protection Office Thematic Review Q4 2023 Outcomes

Oversight Authorities

- National Cyber Security Agency - National Cyber Governance and Assurance Affairs
- Communications Regulatory Authority
- Qatar Central Bank
- Qatar Financial Centre (QFC)

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.

Qatar's data protection law generally supports the free flow of personal data across borders and does not impose broad restrictions. Data controllers are not allowed to restrict cross-border data flows, unless such processing contravenes the provisions of the law or causes significant harm to the data subject.

Specific data transfer conditions apply in the Qatar Financial Centre, which requires equivalent data protection abroad or safeguards such as standard contractual clauses or explicit consent.

Summary

- The Law on Protecting Personal Data Privacy, enacted in 2016 and effective since 2017, generally supports the free flow of data across borders without imposing broad restrictions. The law considers cross-border transfers to include access, retrieval, use and storage of data without state border restrictions.

  The law prohibits data controllers from restricting cross-border data flows, unless such processing contravenes the provisions of the law or causes significant harm to the data subject. The law foresees exceptions to this provision for government bodies, allowing restrictions for reasons such as national security, international relations, economic or financial interests, or criminal investigations.

- The National Cyber Security Agency (NCSA) has introduced a Guidance Booklet on the Law on Protecting Personal Data Privacy. The Booklet emphasises the duty to investigate cross-border data transfers when engaging a third-party processor. Other guidelines focus on data privacy impact assessments, demanding that data controllers conduct impact assessments to identify and mitigate risks associated with the transfer, specifically whether it "may cause serious damage."

  Finally, the guidelines suggest that controllers include details of their data protection compliance measures, including safeguards for international transfers.

- The Cloud Policy Framework by the Communications Regulatory Authority suggests several mechanisms to enable cross-border data flows while protecting privacy and security.

  Specifically, it calls for the following mechanisms to be considered as solutions:

  01. Contractual arrangements;
  02. Alignment with international standards; Binding corporate rules;
  03. Enforceable corporate cross-border privacy rules based on international models;
  04. Certified codes of conduct, certifications, privacy seals and international standards; and
  05. Bilateral or multilateral arrangements based on self-certification.

- The Framework further recommends a data subject consent requirement for personal data transfers.

  In the Qatar Financial Centre (QFC), the Data Protection Regulations and Data Protection Rules allow cross-border data transfers if the QFC's Data Protection Office (DPO) has determined that the recipient jurisdiction offers an adequate level of data protection.

  If not, transfers can still occur if appropriate safeguards are in place, such as standard contractual clauses or explicit consent from the data subject. The DPO has published a Guidance for the Data Protection Regulations and Rules 2021, which provides detailed instructions and best practices for compliance.

SOURCES

Primary Legislation

- Law No. 13 of 2016 on Protecting Personal Data Privacy

Secondary Legislation

- Communications Regulatory Authority: The Cloud Policy Framework
- Qatar Financial Centre: Data Protection Regulations
- Qatar Financial Centre: Data Protection Rules
- Qatar Financial Centre Data Protection Office: List of Adequate Jurisdictions
- Qatar Financial Centre: Standard Contractual Clauses relating to the transfer of Personal Data outside the QFC pursuant to the QFC Data Protection Regulations 2021 ("QFC DPR 2021")

Guidelines

- National Cyber Security Agency: Personal Data Privacy Protection Law Overview
- National Cyber Security Agency: Controller and Processor - Guideline for Regulated Entities
- National Cyber Security Agency: Data Privacy Impact Assessment (DPIA) - Guideline for Regulated Entities
- National Cyber Security Agency: Exemptions Applicable to Competent Authorities (under Article 18) - Guideline for Regulated Entities
- National Cyber Security Agency: Exemptions Applicable to Data Controllers (under Article 19) - Guideline for Regulated Entities
- National Cyber Security Agency: Privacy Notice - Guideline for Regulated Entities
- National Cyber Security Agency: Record of Processing Activities - Guideline for Regulated Entities
- National Cyber Security Agency: Special Nature Processing - Guideline for Regulated Entities
- Qatar Financial Centre: Data Protection Regulations and Rules 2021 Guidance

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.

Qatar does not demand general data localisation, but maintains localisation requirements for specific data and in specific sectors. Regarding government data, Qatar aims to transition to cloud storage and recommends the use of specific providers who have passed residency requirements.

Regarding the financial sector, the Qatar Central Bank requires regulated entities to ensure that personally identifiable information and financial information are processed within Qatar.

Summary

- Qatar generally does not have a general data localisation requirement, allowing businesses to store and process personal data outside the country.

  According to the National Data Classification Policy by the National Cyber Security Agency (NCSA) and the Cloud Policy Framework by the Communications Regulatory Authority (CRA), data residency is no longer required. The National Data Classification Policy introduced data classification and protection guidelines, allowing greater flexibility in data residency requirements.

- The Cloud Policy Framework emphasises that data residency is no longer necessary from an operational perspective, since encryption, anonymisation, aggregation, and certification are more efficient from a security standpoint. Localisation requirements should thus be limited in volume and scope.

  Certain government data is subject to residency requirements. The Cloud First Policy aims to promote government use of cloud services, specifically the transition from on-premise data storage to cloud storage. It recommends the use of "endorsed cloud service providers," which have passed Qatar's data residency, security and operational requirements.

- In addition, data localisation is required in the financial sector. Notably, the Qatar Central Bank (QCB) has issued the Cloud Computing Regulation, which requires QCB-licensed entities to ensure that personally identifiable information and financial information are processed within Qatar. Regulated entities must also obtain approval from the QCB before entering cloud arrangements.

SOURCES

Primary Legislation

- Law No. 13 of 2016 Personal Data Privacy Protection

Secondary Legislation

- National Cyber Security Agency: The National Data Classification Policy
- Communications Regulatory Authority: The Cloud Policy Framework
- Ministry of Communication and Information Technology: Cloud First Policy
- Qatar Central Bank: The Cloud Computing Regulation: Regulating the use of Cloud Computing by QCB-Licensed Entities

Guidelines

- Communications Regulatory Authority: The Cloud Computing Handbook for SME's

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.

The online consumer protection framework comprises the consumer protection law as well as laws on e-commerce, telecommunications, privacy, and competition.

These laws prohibit misrepresentations that mislead consumers, failure to deliver products or provide services after charging consumers, and charging consumers without authorisation, among others.

E-commerce platforms must uphold transparency requirements. Spam is generally forbidden without (express or inferred) consent and must include the contact details of the sender as well as an unsubscribe option. The main oversight authority is the Consumer Protection and Combating Commercial Fraud Department under the Ministry of Commerce and Industry, which is supported by sectoral bodies.

Summary

- The Consumer Protection Law, enacted in 2008, establishes consumer rights, supplier duties, and provisions for creating consumer protection organisations. The law also ensures the protection and privacy of consumer data. Additionally, the Constitution prohibits discrimination based on sex, race, language, or religion. The Executive Regulations of the Consumer Protection Law provide detailed guidance on the law's implementation, ensuring comprehensive consumer rights, prohibiting unfair practices, and defining the obligations of suppliers.

  Online consumer protection is further governed by the E-Commerce and Transactions Law 2010. This law addresses the need for clear identification of entities behind commercial communications and transparency in the nature of online offers, consistent with international standards on electronic messaging.

- Service providers are required to provide consumers with clear and comprehensible terms, including accurate pricing and product descriptions, before orders are placed. **Other relevant laws include:**

01. The Protection of Competition and Prevention of Monopolistic Practices Law, enacted in 2006, which aims to promote fair economic competition and prevent monopolistic practices.
02. The Telecommunication Law, enacted in 2006 and amended in 2017, which includes sections related to consumer protection.
03. The Personal Data Privacy Protection Law, enacted in 2016, which includes consumer protection regarding the transmission of electronic communication for the purpose of direct marketing.

- The Consumer Protection and Combating Commercial Fraud Department, under the Ministry of Commerce and Industry is responsible for overseeing consumer protection. The Department enforces consumer protection laws, handles complaints, starts investigations, and convicts violators. The Ministry has issued several consumer protection guidelines, including those on consumer rights and fraud protection, as well as online shopping.

- For online consumer protection, the Ministry of Communications and Information Technology is empowered to enforce relevant measures against violators.

- Previously, the E-Commerce and Transactions Law 2010 empowered the Supreme Council of Information and Communication Technology (ictQATAR), but the Council was reorganised and its functions were integrated into the Ministry of Communications and Information Technology (MCIT).

  Other authorities include the Qatar Central Bank for the financial sector and the Communications Regulatory Authority for the telecommunications sector. **For example, the Communications Regulatory Authority has issued:**

01. The Consumer Protection Policy, establishing standards for telecommunications consumer rights,
02. The Code on Advertising, Marketing and Branding, protecting consumers from misleading and anticompetitive advertisements; and
03. The Spam Regulation, outlining obligations for service providers, senders, and users of electronic communications for direct marketing.

- The former Ministry of Transport and Communications, whose responsibilities related to communications were transferred to the Ministry of Communications and Information Technology (MCIT), issued the E-Commerce Guidelines Terms & Conditions.

  They provide a framework for e-commerce businesses in Qatar to follow best practices, ensure compliance with international standards, and protect consumer rights.

  Finally, the Qatar Financial Centre Regulatory Authority issues consumer protection guidelines on its official website, including scam detection, dispute resolution, and a consumer alert bulletin.

  The Authority further provides a no-cost customer dispute resolution scheme between customers and authorised firms.

SOURCES

Primary Legislation

- Law No. 8 of 2008 on Consumer Protection
- E-Commerce and Transactions Law No.16 of 2010
- - Qatar Constitution, Article 35 regarding Non-Discrimination
- Law No. 19 of 2006 on the Protection of Competition and Prevention of Monopolistic Practices
- The Telecommunication Law No. 34 2006 Amended Provisions No. 17 2017
- The Law No.13 of 2016 Personal Data Privacy Protection

Secondary Legislation

- Ministry of Commerce and Industry: Executive Regulation of Law No. 8 of 2008 on Consumer Protection
- Communications Regulatory Authority: The Consumer Protection Policy
- Communications Regulatory Authority: Spam Regulation (Amended)
- Communications Regulatory Authority: Code on Advertising, Marketing and Branding
- Amiri Decree No. 47 of 2022 on the organisational structure of the Ministry of Communications and Information Technology

Guidelines

- Ministry of Commerce and Industry: The Consumer Rights Guide
- Ministry of Commerce and Industry: We combat fraud and protect your rights
- Ministry of Commerce and Industry: Shop online when you are ready
- Ministry of Commerce and Industry: Policy and mechanism of exchange and return
- Ministry of Commerce and Industry: Safe online shopping
- Qatar Financial Centre: Regulatory Authority Scam detection guidelines
- Qatar Financial Centre: Regulatory Authority Investment Considerations
- Qatar Financial Centre: Regulatory Authority Consumer Alert Bulletin
- Qatar Financial Centre: Regulatory Authority Customer Dispute Resolution Scheme
- Ministry of Transport and Communications: E-Commerce Guidelines Terms & Conditions

Oversight Authorities

- The Consumer Protection and Combating Commercial Fraud Department under the Ministry of Commerce and Industry
- Ministry of Communications and Information Technology
- Qatar Central Bank
- Communications Regulatory Authority
- Qatar Financial Centre Regulatory 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.

Qatar's law on electronic commerce and transactions emphasises the validity and enforceability of electronic communications to conduct transactions. Exceptions concern transactions concerning family and personal status, among others.

Qatar establishes the legal validity of electronic signatures, albeit without differentiating different types of signatures. Foreign-issued electronic signatures have the same legal effect as domestic ones, if they offer the same level of reliability.

Finally, Qatar accepts electronic authentication and offers a governmental authentication service (Tawtheeq) to verify the digital identity of the users of e-government services.

Summary

- The Decree Law on the Promulgation of the Electronic Commerce and Transactions Law primarily governs electronic transactions. This law sets out the framework for recognising and enforcing electronic transactions and provides the legal basis for electronic signatures and electronic documents. Under this law, electronic transactions are recognised as equivalent to paper-based transactions, with certain exceptions. Specifically, electronic communications can be used for contract formation and transactions, and these are not invalidated solely due to their electronic nature. However, the law excludes certain documents and transactions, including those related to family and personal status. Notably, documents related to land transactions and notarial documents were removed from the exclusions by Cabinet Resolution.

- The decree law recognises a single category of electronic signatures, which must meet specific criteria to have evidential weight. These criteria include ensuring that the signature creation information is uniquely associated with the signatory, remains under their control at the time of signing, and that any alterations to the signature of the information it relates to are detectable. The Ministry of Communications and Information Technology is responsible for determining which electronic signatures processes and technologies meet these requirements. Additionally, the law stipulates that foreign-issued electronic signatures are recognised in Qatar if they offer a level of reliability equivalent to that required by Qatari law.

  Electronic authentication is permitted in Qatar and is governed by similar principles as those for electronic signatures. Electronic authentication must adhere to criteria ensuring integrity and security of the signed or authenticated information. The Ministry of Communications and Information Technology will decide on the processes and technologies that fulfil these requirements. Additionally, the decree law allows parties to agree on the use of specific certification certificates as long as the agreement complies with legal standards. The National Authentication Service, known as Tawtheeq, is managed by the Ministry of Communications and Information Technology. It is the national system designed to verify the digital identity of individuals and businesses using e-government services, providing a governmental authentication service that supports private transactions.

- The Ministry of Communications and Information Technology (MCIT) has issued the Qatar Digital Government 2020 Strategy, Qatar Digital Government Strategy 2023-2025, Digital Agenda 2030, and the Electronic Commerce and Transaction Policy. The latter sets binding rules for e-commerce within the TASMU Ecosystem, a digital transformation initiative launched by Qatar to enhance the use of technology and data across various sectors. The Qatar Central Bank (QCB) has also introduced binding regulations, such as the Payment Services Regulation, which contains aspects related to e-transactions including the secure use of e-signatures.

- In addition to these regulations, several guidelines have been issued. The MCIT published the Qatar National E-Commerce Roadmap and various guidelines, including the E-Commerce Technology Guidelines, and the E-Commerce Security Guidelines, which help Qatar's eMerchants adhere to best practice in e-commerce. Moreover, the Communications Regulatory Authority (CRA) has issued Qatar's ICT Landscape & Digital Trends 2022. Finally, the Ministry of Interior (MOI) provides the Qatar Digital ID (QDI) mobile app for identity verification and access to electronic services.

SOURCES

Primary Legislation

- Decree Law No. 16 of 2010 on the Promulgation of the Electronic Commerce and Transactions Law
- Secondary Legislation
- Cabinet Resolution No. 1 of 2019 amending the exceptions to some documents and papers stipulated in the Electronic Transactions and Commerce Law issued by Decree-Law No. 16 of 2010
- Ministry of Communications and Information Technology: Electronic Commerce and Transaction Policy
- Qatar Central Bank: Fintech Strategy in State of Qatar
- Qatar Central Bank: Payment Services Regulation

Guidelines

- Ministry of Communications and Information Technology: Qatar Digital Government Strategy 2023-2025
- Ministry of Communications and Information Technology: Qatar e-Government 2020 Strategy
- Ministry of Communications and Information Technology: Digital Agenda 2030
- Ministry of Transport and Communications: Qatar National E-Commerce Roadmap 2017
- Ministry of Transport and Communications: E-Commerce Technology Guidelines
- Ministry of Transport and Communications: E-Commerce Terms and Conditions Guidelines
- Ministry of Transport and Communications: The E-Commerce User Experience Guidelines
- Ministry of Transport and Communications: The E-Commerce User Interface Design Guidelines
- Ministry of Transport and Communications: The E-Commerce Security Guidelines
- Communications Regulatory Authority: Qatar's ICT Landscape & Digital Trends 2022
- Qatar Digital ID Card

Oversight Authorities

- Ministry of Communications and Information Technology
- Ministry of Communications and Information Technology - National Authentication Service

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.

Qatar provides trade administration documents for imports in electronic form, in both Arabic and English, and accepts electronic submissions. The Electronic Customs Clearance "Single Window" (Al Nadeeb Clearance system) is operational and supports international data and document exchange. Finally, Qatar expedites customs procedures for low-value shipments, since it exempts personal shipments valued below QAR 1000.

Summary

- Qatar has established a comprehensive legal framework to support the transition to paperless trade, with a focus on customs procedures and electronic documentation.

  The Customs Law of 2002 governs customs procedures in Qatar, and amended to accommodate electronic documentation and processes. As a member of the Gulf Cooperation Council (GCC), Qatar implements the Unified Customs Law of the GCC States, which allows for the submission of electronic customs declarations and documents, thereby facilitating paperless trade processes.

- To further streamline customs procedures, Qatar exempts personal shipments valued under QAR 1000 from customs duties.

  The Electronic Commerce and Transactions Law, enacted in 2010, provides the legal foundation for recognising electronic documents and signatures, which are essential for paperless trade. Secondary legislation includes the Executive Regulations of the Customs Law, which outline the operational aspects of customs procedures, including the acceptance of electronic trade documents.

- The General Authority of Customs has developed several official guidelines and documents to facilitate paperless trade through the electronic single window (Al Nadeeb Clearance system). These guidelines include registration procedures, detailed instructions for customs clearing agents, traders, shipping agents, and other government agencies. Additionally, there are specific guides on managing detained goods, handling operations in bonded warehouses, and addressing financial claims related to additional payments. Qatar's approach to paperless trade is informed by international frameworks, such as the WTO's Trade Facilitation Agreement (TFA) and the WCO's SAFE Framework of Standards. These guidelines ensure that Qatar's systems are compatible with global best practices, thereby enhancing the efficiency and competitiveness of the country's trade environment. This aligns with Qatar's Electronic Commerce and Transactions Law, which is influenced by international frameworks such as the UNCITRAL Model Law, providing a legal foundation for recognising electronic communications, documents, and electronic signatures in international trade.

- In the regional context, Qatar adheres to the Gulf Cooperation Council (GCC) Unified Customs Law, which facilitates the digitalisation of customs procedures across GCC member states and supports the integration of electronic systems for customs and trade documentation. Furthermore, Qatar is part of the Agreement on Facilitation and Development of Trade Exchange concluded between Arab countries, which aims to enhance and streamline trade among its member states.

- In addition to these multilateral commitments, Qatar has entered into bilateral agreements with individual countries to further simplify customs procedures and boost trade. These agreements typically include provisions for mutual recognition of customs documentation, reduced tariffs on certain goods, and enhanced cooperation in customs enforcement.

SOURCES

Primary Legislation

- Law No. 40 of 2002 issuing the Customs Law
- Law No. 10 of 2023 amending some provisions of the Customs Law issued by Law No. 40 of 2002
- Decree Law No. 16 of 2010 on the Promulgation of the Electronic Commerce and Transactions Law

Secondary Legislation

- Cabinet Resolution No. 21 of 2004 issuing the Executive Regulations of the Customs Law
- Cabinet Resolution No. 9 of 2013 amending some provisions of the Executive Regulations of the Customs Law issued by Cabinet Resolution No. 21 of 2004
- Minister of Finance Decision No. 13 of 2023 determining the fees for customs services provided by the General Authority of Customs

Guidelines

- General Authority of Customs: The Registration Guide
- General Authority of Customs: The QCCSW for Customs Clearing Agents
- General Authority of Customs: The QCCSW for Traders
- General Authority of Customs: The QCCSW for Shipping Lines/Agents
- General Authority of Customs: The QCCSW for Other Government Agencies (OGA)
- General Authority of Customs: The Customs Clearing Agent Guide - Detained Goods
- General Authority of Customs: The Government Agencies Guide - Detained Goods
- General Authority of Customs: The Clearance Agent Guide - Bonded Warehouses
- General Authority of Customs: The Clearance Agent Guide - Additional Payment Financial Claims
- General Authority of Customs: For Individuals - Exemption of parcels and personal mailings whose value does not exceed (1000) riyals

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.

Qatar has enacted a law dedicated to preventing cybercrime, complemented by several regulations by the National Cyber Security Agency and the central bank. Penalties are based on the nature and impact of cybercrimes. The National Data Classification Policy establishes five data levels and imposes security and risk assessment obligations by level.

Cybersecurity incidents must be reported to authorities. The National Cyber Security Agency, which reports directly to the Council of Ministers, is responsible for oversight, along with other sectoral and central government bodies.

Summary

- The Cybercrime Prevention Law was enacted and has been in effect since 2014. It covers a broad spectrum of cybercrimes, including unauthorised access, hacking, cyber-stalking, data theft, malware distribution, child exploitation, and cyber-terrorism. The law obliges internet service providers to implement preventive measures and collaborate with authorities during investigations.

  Additionally, controllers must report personal data breaches to the National Cyber Governance and Assurance Affairs at the National Cyber Security Agency (NCSA) and notify affected individuals within 72 hours of becoming aware of it.

- The NCSA oversees cybersecurity in Qatar, ensuring compliance with national standards, developing strategies and assessing cyber risks. The NCSA reports directly to the Council of Ministers, indicating its role in high-level policy and strategic oversight. The Economic and Cyber Crimes Combating Department, under the Ministry of Interior, enforces the Cybercrime Prevention Law, focusing on the operational aspects of cybersecurity.

- This includes monitoring, investigating, and prosecuting cybercrimes. The Public Prosecution works in coordination with the Ministry of Interior to investigate and prosecute these crimes. It has the authority to conduct inspections, seize devices, and gather evidence. Other relevant authorities include the Communications Regulatory Authority for the telecommunications sector and the Qatar Central Bank for the financial sector.

  The NCSA has issued several regulations such as the Qatar Cyber Security Framework, the National Data Classification Policy, and the National Information Assurance Standard. These regulations

- provide detailed standards to enhance cybersecurity measures, ensure compliance, protect critical information infrastructure across the nation, and align with the Qatar National Cyber Security Strategy. Additionally, the Qatar Central Bank has issued the Cyber Security Circular 2016, the Cyber Security Regulation for Payment Service Providers, and the Insurance Sector Cyber Security Regulation to enhance the resilience of financial institutions against cyber threats, ensuring robust protection of sensitive data and maintaining the integrity of financial transactions. They mandate stringent security measures, regular audits, and comprehensive incident response plans to safeguard the financial ecosystem.

- The NCSA has issued a series of guidelines covering cybersecurity, such as ransomware attacks, distributed denial of service (DDoS) attacks, securing social media accounts, public Wi-Fi networks, and hotel information systems. These guidelines provide best practices and actionable steps to mitigate risks and enhance cybersecurity posture across various sectors. Additionally, the central bank launched the 'Stay Aware' campaign in cooperation with the Ministry of Interior, National Cybersecurity Agency, and the Qatar Financial Centre Regulatory Authority. This campaign aims to educate the public on the dangers of financial fraud and cyber threats.

SOURCES

Primary Legislation

- Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law

- **Secondary Legislation**
- National Cyber Security Agency: The Qatar Cyber Security Framework [source not working]
- National Cyber Security Agency: The National Data Classification Policy [source not working]
- National Cyber Security Agency: The National Information Assurance Standard [source not working]
- Qatar Central Bank: The Cyber Security Circular Regarding Technology Risks
- Qatar Central Bank: The Information and Cyber Security Regulation for Payment Service Providers
- Qatar Central Bank: The Insurance Sector CyberSecurity Regulation

Guidelines

- Ministry of Information and Communications Technology: The Qatar National Cyber Security Strategy
- National Cyber Security Agency: Personal Data Breach Notifications - Guideline for Regulated Entities
- National Cyber Security Agency: Guidelines Ransomware Attacks [source not working]
- National Cyber Security Agency: Guidelines Distributed Denial of Service Attacks [source not working]
- National Cyber Security Agency: Securing Social Media Accounts [source not working]
- National Cyber Security Agency: Guidelines Public Wi-Fi Networks [source not working]
- National Cyber Security Agency: Guidelines Hotels Information Systems [source not working]

Oversight Authorities

- The National Cyber Security Agency [source not working]
- The Economic and Cyber Crimes Combating Department under the Ministry of Interior
- The Public Prosecution [source not working]
- Communications Regulatory Authority
- Qatar Central Bank

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.

Qatar does not have a specific regulatory framework for AI but is currently developing AI guardrails. Accordingly, neither risk-based nor technology-based rules apply to AI providers. The government has issued a national AI strategy, aiming to drive innovation in line with the Qatar National Vision 2030, as well as guidelines for the secure adoption and usage of AI. In addition, the government has established an AI Committee under the Ministry of Communications and Information Technology. Most recently, the Qatar Central Bank issued an AI Guideline for licensed entities.

Summary

- Qatar is reportedly in the process of establishing a specific regulatory framework for AI but does not currently impose AI obligations. AI is primarily overseen by the Ministry of Communications and Information Technology (MCIT), which has the authority to draft rules. The Artificial Intelligence Committee, established within the MCIT in 2021, is responsible for implementing Qatar's National AI Strategy. Additionally, the Civil Service and Government Development Bureau is working on developing laws, including those regulating AI use, and ensuring effective communication between the public and private sectors and the Qatari legislature.

- The MCIT has issued the National AI Strategy, aiming to position the country as a leader in AI. This strategy focuses on six pillars: education, data access, employment, business, research, and ethics, with the goal of driving innovation and aligning with Qatar National Vision 2030.

  The strategy also highlights the need for easy yet well-regulated data access to foster innovation and recommends developing a stable regulatory framework to make Qatar an attractive hub for AI-driven businesses globally. Additionally, MCIT has issued principles and guidelines for ethical use AI use, including six principles:

  01 Safeguard personal and organisational data,
  02 Comply with relevant laws and regulations,
  03 Ensure the well-being of individuals and Society,
  04 Assume accountability,
  05 Acknowledge AI's capabilities and limitations,
  06 Do not use AI systems to perpetuate bias.

- In addition, MCIT issued guidelines on the ethical development and deployment of AI, encompassing eight principles: do no harm, ensure system robustness, security, and safety, avoid perpetuating bias and discrimination, protect the environment, safeguard privacy, promote transparency, develop a human-centred approach, and assign ultimate accountability to humans).

- The National Cyber Security Agency (NCSA) also plays a role in overseeing AI applications from a cybersecurity perspective, focusing on the security implications of AI technologies. In addition, the Guidelines for Secure Adoption and Usage of Artificial Intelligence, issued by the NCSA, outline best practices for AI deployment across all public and private organisations. This guideline emphasises secure AI practices and is designed to support organisations using or planning to deploy AI systems, services, or products.

- The Qatar Central Bank oversees the integration of AI within the financial sector. The bank recently issued the AI Guideline, effective from September 2024, to regulate the use of AI by licensed entities. Such entities must develop an AI strategy aligned with their needs and risk appetite, consistent with internal policies. In addition, board directors and senior management are accountable for the outcomes and decisions of AI systems, including those operating autonomously.

  The Ministry of Public Health oversees AI within the healthcare sector, ensuring that AI-driven medical technologies and services comply with ethical standards and patient safety regulations.
  Within the Qatar Financial Centre, the Qatar Financial Centre Regulatory Authority oversees and regulates the use of AI in financial services.

SOURCES

Guidelines

- Ministry of Communications and Information Technology: The National Artificial Intelligence Strategy
- Ministry of Communications and Information Technology: Artificial Intelligence in Qatar - Principles and Guidelines for Ethical Development and Deployment
- Ministry of Communications and Information Technology: Artificial Intelligence in Qatar- Principles and Guidelines for Ethical Use
- National Cyber Security Agency: Guidelines for Secure Adoption and Usage of Artificial Intelligence
- Qatar Central Bank: AI Guideline

News reports on AI regulation

- Qatar Day: MCIT Crafting AI Regulation to Tackle Ethical and Legal Issues [third party news source]
- Gulf Times: QCB plans to issue first guidelines on how to adapt AI: Sheikh Bandar [third party news source]

Oversight Authorities

- Ministry of Communications and Information Technology
- The Artificial Intelligence Committee
- Civil Service and Government Development Bureau
- Qatar Central Bank
- Ministry of Public Health
- Qatar Financial Centre Regulatory Authority

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 for "computer programs," classifying them as literary works and granting authors the exclusive rights over the reproduction, distribution, and adaptation of source code. Exceptions are foreseen for "fair use," including personal, educational, and research purposes. Source code sharing is not generally mandated. Sectoral regulations, on insurance and banking, require providers to review the source code of "critical applications" to identify vulnerabilities. Otherwise, providers are encouraged to acquire or arrange an escrow for the source code.

Summary

- Source code is protected under the country's Intellectual Property framework, specifically under the Law on Protection of Copyright and Neighboring Rights (Qatar Copyright Law). This law grants authors exclusive rights of computer programs, including source code. These programs are treated as literary works.
  Qatar's copyright law also includes fair use exceptions, allowing limited reproduction, translation, or quotation of works for personal, educational, or research purposes, as long as it does not conflict with normal usage or harm the legitimate interests of the author.

- While there is no general requirement for companies to share source code to access the market, certain sectors, particularly those related to critical infrastructure, may face such requirements due to national security concerns. For instance, the National Information Assurance Standard recommends that the source code of custom-developed critical applications be made available. For commercial applications serving critical processes, the standard suggests that organisations investigate escrow options to ensure the source code is accessible under specific conditions.

  Specific sectors like banks and insurance have explicit requirements regarding source code. Both are required to perform source code reviews to detect vulnerabilities caused by coding issues, poor practices, or malicious attempts. They are also expected to acquire the source code for custom-developed critical applications, or if acquisition is not feasible, investigate escrow options to ensure access.

- The public policy objectives behind these regulations include ensuring national security, maintaining cybersecurity standards, and promoting consumer protection. These measures aim to secure critical infrastructure, protect digital systems from cyber threats, and ensure software reliability for public use.

SOURCES

- Law No. 7 of 2002 on the Protection of Copyright and Neighbouring Rights
- National Cyber Security Agency: National Information Assurance Standard [source not working]
- Qatar Central Bank: Cyber Security Circular Regarding Technology Risks
- Qatar Central Bank: Insurance Sector Cyber Security Regulation

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.

For digital services or digital products, Qatar imposes neither customs duties nor indirect taxes, although it is laying the foundation for a value-added-tax of 5%. For e-commerce imports, Qatar applies customs duties, but no indirect taxes. Qatar does not have a specific direct tax targeting providers of digital services or digital products, relying instead on its existing corporate income tax framework. Qatar's General Tax Authority and Customs Authority provide online portals for registration, compliance, and customs clearance.

Summary

- Qatar applies customs duties on goods imports, including e-commerce imports, but not services. E-commerce imports are subject to standard customs duties. General goods such as clothing, electronics, and cars face a 5% duty, while some categories like steel incur higher duties. Goods for personal use with a value not exceeding QAR 1,000 are exempt from import duties. The Customs Law, enacted in 2002, regulates import and export activities, detailing customs procedures.

- The Executive Regulations of the Customs Law specifies procedures for customs clearance, duties, and inspections. The General Authority of Customs oversees and enforces customs regulations related to imports, exports, and e-commerce. The General Authority of Customs has issued several guidelines, including on customs clearance and procedures.

- Qatar does not impose value-added-tax. Qatar is a signatory to the GCC VAT Framework, which mandates the eventual introduction of VAT at a standard rate of 5% on physical and digital goods and services. In addition, The Excise Tax Law 2018 governs the excise tax on specific goods, including tobacco, carbonated drinks, and energy drinks. The Executive Regulations of the Excise Tax Law, outline the processes for administering excise taxes on designated goods.

- Qatar does not currently impose direct taxes specifically on providers of digital services or digital products, instead relying on corporate income tax. Taxable income is generally subject to a flat tax rate of 10%, although there are certain exceptions.

- The Income Tax Law, enacted in 2018 and amended in 2022, establishes regulations for corporate income tax, withholding tax, and related provisions. The Executive Regulations of the Income Tax Law provide operational procedures for tax filing, payment, and compliance requirements. The General Tax Authority administers the tax regime and provides online services through the Dhareeba Tax Portal.

- As a member of the Gulf Cooperation Council (GCC), Qatar implements the Unified Customs Law of the GCC States to harmonise customs regulations regionally. In addition, Qatar is a long-time member of the World Customs Organization and the GCC Customs Union.

- Finally, Qatar entered into several bilateral tax treaties and is a signatory of the Organisation for Economic Co-operation and Development Multilateral Agreement to Combat Base Erosion and Profit Shifting and the Agreement on Mutual Administrative Assistance in Tax Matters.

- The Qatar Financial Centre (QFC) Tax Department governs taxation for firms operating under the QFC regime, imposing a 10% tax on the local source profits of firms licensed by the QFC, although there are exceptions.

SOURCES

Primary Legislation

- Law No. 24 of 2018 Promulgating the Income Tax Law 24/2018
- Law No. 11 of 2022 Amending Several Provisions of Income Tax Law Promulgated by Law No. 24 of 2018
- Law number 25 of 2018 on Excise Tax
- Law No. 40 of 2002 promulgating the Customs Law
- Law No. 10 of 2023 amending some provisions of the Customs Law issued by Law No. 40 of 2002
- Law No. 41 of 2002 Amending the Customs Tariff and Cancelling Some Customs Exemptions

Secondary Legislation

- The Executive Regulations of the Income Tax Law promulgated by Law No. 24 of 2018
- The Executive Regulations of Law number 25 of 2018 on Excise Tax
- Council of Ministers Resolution No. 21 of 2004 on issuing the Executive Bylaw of the Customs Law
- Council of Ministers Decision No. 9 of 2013 amending certain provisions of the Executive Regulations of the Customs Law issued by Council of Ministers Decision No. 21 of 2004
- Minister of Finance Decision No. 13 of 2023 determining the fees for customs services provided by the General Authority of Customs
- Qatar Financial Centre Tax Regulations
- Qatar Financial Centre Tax Rules

Guidelines

- General Tax Authority: Taxes in Qatar
- General Tax Authority: FAQ
- General Authority of Customs: The Standard Guide for Clearing Requirements of Imported Goods
- General Authority of Customs: The Unified Guide for Customs Procedures
- General Authority of Customs: The Customs amount Guide
- General Authority of Customs: The Customs broker's guide
- General Authority of Customs: The Single Window Project Guide
- General Authority of Customs: The Traveler's Guide
- General Authority of Customs: The General Authority of Customs - Publications
- General Authority of Customs: For Individuals - Exemption of parcels and personal mailings whose value does not exceed (1000) riyals
- Qatar Financial Centre: Tax Manual
- Qatar Financial Centre: e-Services User Guide - Tax
- Qatar Financial Centre: Tax Return Completion Guide

International Frameworks

- The Common Customs Law of the GCC States
- The Common Customs Law of the GCC States - Rules of Implementation And Explanatory Notes Thereof
- The Common VAT Agreement of the States of the Gulf Cooperation Council (GCC)
- Tax agreements
- Invest Qatar - Laws And Regulations – Customs – Customs Overview
- The Common Customs Law of the GCC States
- The GCC Customs Union

Oversight Authorities

- General Tax Authority
- General Authority of Customs
- Qatar Financial Centre Tax Department

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.

Qatar's regulatory framework for digital payments draws from several laws that are not digital-specific, including the laws on the regulation of financial institutions and on anti-money laundering and terrorism financing. These laws establish know-your-customer, anti-money-laundering, and counter-terrorism-financing rules. In addition, no financial services can be delivered without a licence from the central bank. For cross-border wire transfers, the framework demands the name of the originator and the beneficiary, as well as both account numbers or a unique transaction reference number, for traceability. Beneficiary financial institutions must identify transfers that lack the required information and, for transfers above QR 3,500, verify the identity of the beneficiary.

Summary

- The Qatar Central Bank (QCB) Law of 2012, provides the QCB with the authority to regulate financial institutions, including those dealing with digital payments in the private sector.

- The Combating Money Laundering and Terrorism Financing Law, enacted in 2019, applies to financial institutions and designated non-financial businesses and professions, including digital payment service providers. It mandates compliance with know your customer (KYC), anti-money laundering (AML), and combating the financing of terrorism (CFT) procedures.

- The Electronic Transactions and Commerce Law of 2010, validates electronic transactions and signatures within payment systems. Additionally, the Cybercrime Law of 2014, addresses cyber crimes related to digital payments, including fraud and unauthorised access.

- The Implementing Regulations of the Combating Money Laundering and Terrorism Financing Law provide detailed requirements for KYC, AML, and CFT compliance by digital payment providers.

  The Ministry of Communications and Information Technology (MCIT) has issued the Qatar Digital Government 2020 Strategy, Qatar Digital Government 2023-2025 Strategy, Digital Agenda 2030, and the Electronic Commerce and Transaction Policy. The strategy aims to digitise all government services, including payment services, while the policy sets the rules and regulations for electronic commerce within the TASMU Ecosystem, a digital transformation initiative launched to enhance the use of technology and data across sectors. The Qatar Central Bank has issued several regulations directly related to digital payments. These include the Payment Services Regulation, which governs digital payment services such as e-money issuance, merchant acquiring services, and local fund transfer services.

- The Information and Cyber Security Regulation for Payment Service Providers, which mandates that payment service providers implement cybersecurity measures to protect against threats such as fraud, unauthorised access, and data breaches. The Buy-Now-Pay-Later Regulation pertains to digital payment methods that allow consumers to make purchases and pay for them over time.

- Additionally, the E-KYC Regulation is crucial for digital payment systems, as it involves electronic processes to verify the identity of users and ensure compliance with anti-money laundering and combating the financing of terrorism requirements. These regulations are part of the broader Qatar FinTech Strategy 2023, which aims to enhance the digital payment ecosystem and support the transition towards a cashless economy.

- The Qatar Central Bank (QCB) continuously publishes and updates guides on its website regarding Large Value Payment Systems and Retail Payment Systems, including electronic payments and settlement systems. The Third Financial Sector Strategic Plan, issued by the QCB in 2023, focuses significantly on digital payments. The strategy aims to develop a robust digital finance ecosystem, enhance advanced payment solutions like digital wallets and virtual cards, and establish a payment hub with real-time transaction monitoring and fraud detection.

- These initiatives support the transition to a cashless economy and align with Qatar's National Vision 2030.

- Qatar is actively engaged in several international frameworks concerning digital payments, ensuring that its financial systems align with global standards for security, compliance, and interoperability. Qatar also adopts international standards such as ISO/IEC ensuring its digital payment systems are both secure and compatible with global platforms. Participation in the SWIFT network further enhances Qatar's ability to manage cross-border payments, which is essential for international business and remittances. Also, Qatar is a member of the IBAN system.

  The Qatar Central Bank mandated the use of IBAN for all bank accounts in Qatar which helps facilitate international and domestic payments by ensuring that bank account numbers are standardised and easily recognizable across borders.

- In addition, Qatar collaborates with international bodies like the International Monetary Fund (IMF) and the World Bank to promote financial stability, inclusion, and technological innovation in its payment systems. Furthermore, Qatar's alignment with guidelines from the United Nations and the International Telecommunication Union (ITU) reflects its focus on secure digital financial services and financial inclusion.

- Moreover, Qatar's commitments under the World Trade Organization (WTO) support the development of digital payment systems that are compatible with international trade practices.
  On a regional level, Qatar is actively involved with the Arab Monetary Fund (AMF) and the Buna Payment Platform, as well as the Gulf Cooperation Council (GCC) framework to harmonise payment systems and regulations. Finally, Qatar has also established the GCCNET, a single ATM network linking all the GCC National Switches.

SOURCES

Primary Legislation

- Law No. 13 of 2012 on Issuing the Law on Qatar Central Bank and the Regulation of Financial Institutions
- Law No. 20 of 2019 on the Promulgation of Anti-Money Laundering and Terrorism Financing Law
- Decree Law No. 16 of 2010 on the Promulgation of the Electronic Commerce and Transactions Law
- Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law

Secondary Legislation

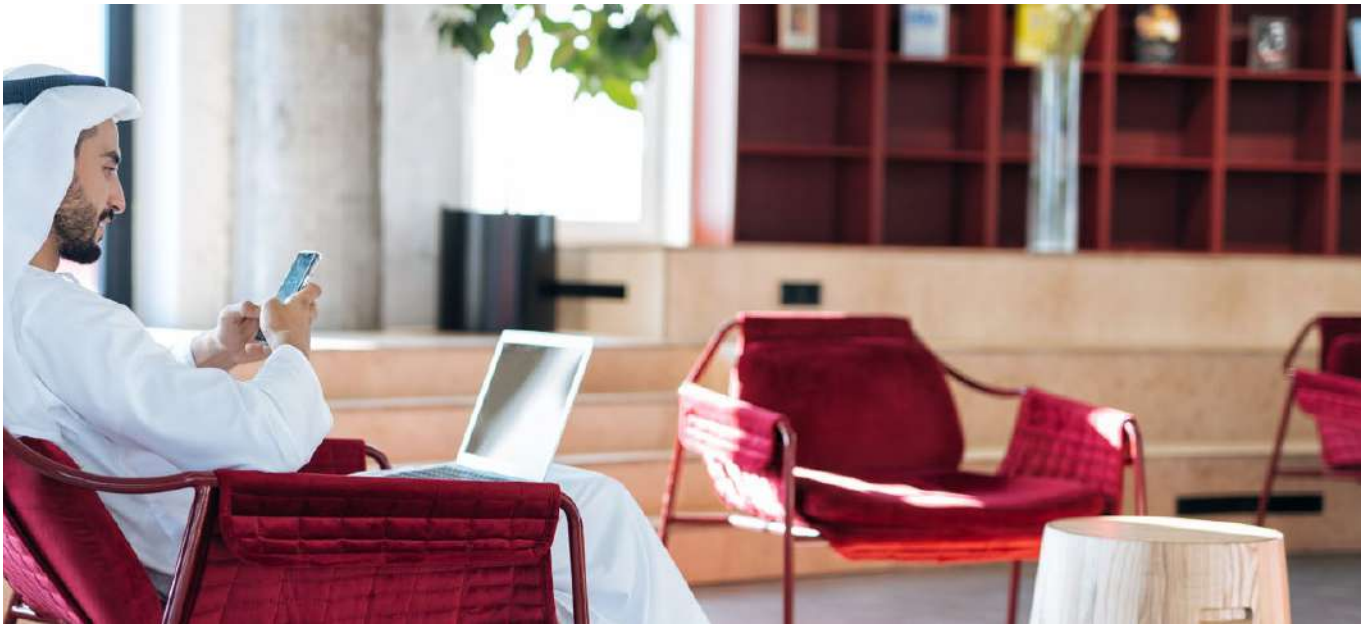
- Council of Ministers' Decision No. 41 of 2019 Promulgating the Implementing Regulations of Law No. 20 of 2019 on Combating Money Laundering and Terrorism Financing
- Ministry of Communications and Information Technology: Electronic Commerce and Transaction Policy
- Qatar Central Bank: Fintech Strategy in State of Qatar
- Qatar Central Bank: Payment Services Regulation
- Qatar Central Bank: The Circular no.: 1/2024 Regarding Amendment to Article No. 5 of the Payment Services Regulation
- Qatar Central Bank: Information and Cyber Security Regulation for Payment Service Providers
- Qatar Central Bank: Buy-Now-Pay-Later Regulation
- Qatar Central Bank: E-KYC Regulation

Guidelines

- Ministry of Communications and Information Technology: Qatar Digital Government Strategy 2023-2025
- Ministry of Communications and Information Technology: Qatar e-Government 2020 Strategy
- Ministry of Communications and Information Technology: Digital Agenda 2030
- Qatar Central Bank: Third Financial Sector Strategic Plan
- Qatar Central Bank: Large Value Payment Systems
- Qatar Central Bank: Retail Payment Systems
- Qatar Central Bank: electronic payments and settlement systems

International Frameworks

- The Financial Action Task Force
- The International Bank Account Number (IBAN) - QATAR
- The International Monetary Fund List of Members
- The World Bank Member Countries
- The Buna payment Platform
- The GCCNET
- The AFAQ Gulf payments system
- The ITU Member States
- The United Nations Member States
- The WTO | Qatar - Member information



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. Qatar has implemented a range of initiatives to support SMEs and disadvantaged groups in accessing digital trade opportunities. T

hese efforts, guided by the Qatar National Vision 2030 and the subsequent Digital Agenda 2030, encompass various programmes offering technical assistance, financial support, and digital infrastructure development. The initiatives span from broad-based SME support to sector-specific digital transformation efforts.

2

Summary

- The Ministry of Communications and Information Technology (MCIT) leads several programmes targeting SMEs' digital capabilities. The Digital Transformation of SMEs programme provides technical assistance for e-commerce integration and digital technology adoption, alongside preferential terms from approved service providers. Complementing this, the MCIT's Business Connect Program offers digital capability workshops and advisory services to SMEs.

- Qatar's E-commerce portal, launched in 2019, serves as a centralised platform providing SMEs with information, tools, and support for international sales. This initiative aligns with the 2017 E-Commerce Roadmap and emphasises accelerating e-commerce adoption among SMEs. The associated Theqa eTrustmark certification system aims to enhance the credibility of online vendors, including SMEs.

  The Qatar Development Bank (QDB) contributes to SME digital transformation through its "Financing Technology and Digital Solutions" programme. This initiative offers Qatar-based SMEs preferential financing for up to 85% of the cost of acquiring technology solutions. QDB supplements this financial support with technology expert advice and digital transformation workshops.

- To further enhance SME digital capabilities, QDB has established partnerships with private sector entities. The collaboration with Ooredoo through the Digital Factory Once programme and the partnership with Microsoft both focus on providing skill-building support and digitisation services to SMEs.

- The Qatar Smart Program (TASMU), launched in 2017, represents a broader digital transformation initiative with potential benefits for SMEs. While not exclusively targeted at SMEs, TASMU's Connected Farmer theme illustrates how the programme supports specific sectors. This theme facilitates farmers' adoption of smart technologies and provides access to an online marketplace connecting farmers directly with end buyers.

SOURCES

- Qatar National Vision 2030
- Digital Agenda 2030
- Ministry of Communications and Information Technology: Digital Transformation of SMEs
- Ministry of Communications and Information Technology: Business Connect Program
- Ministry of Communications and Information Technology: Qatar's eCommerce portal
- Qatar National E-Commerce Roadmap 2017
- Theqa eTrustmark
- Qatar Development Bank: Technology and Digitalization Solution Financing
- Qatar Development Bank: QDB and Microsoft Joint Initiative
- Qatar Development Bank: Digital Factory One
- TASMU: Connected Farming

02
Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Qatar'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 Qatar'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 24.99% of Qatar's imports. The share of advanced technology products in exports was considerably lower at 0.39%, indicating a significant technology trade imbalance.

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

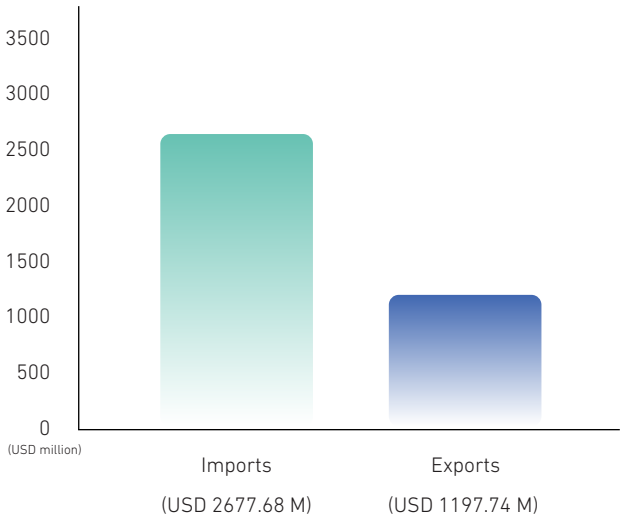


Figure 1 provides data for Qatar's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

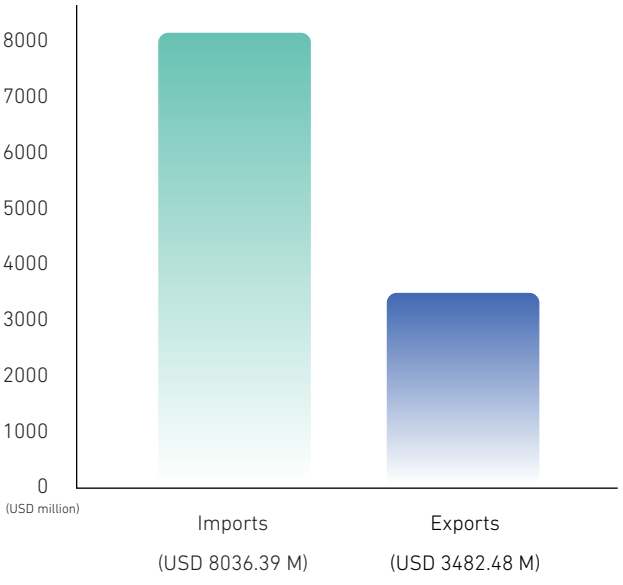


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Qatar'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

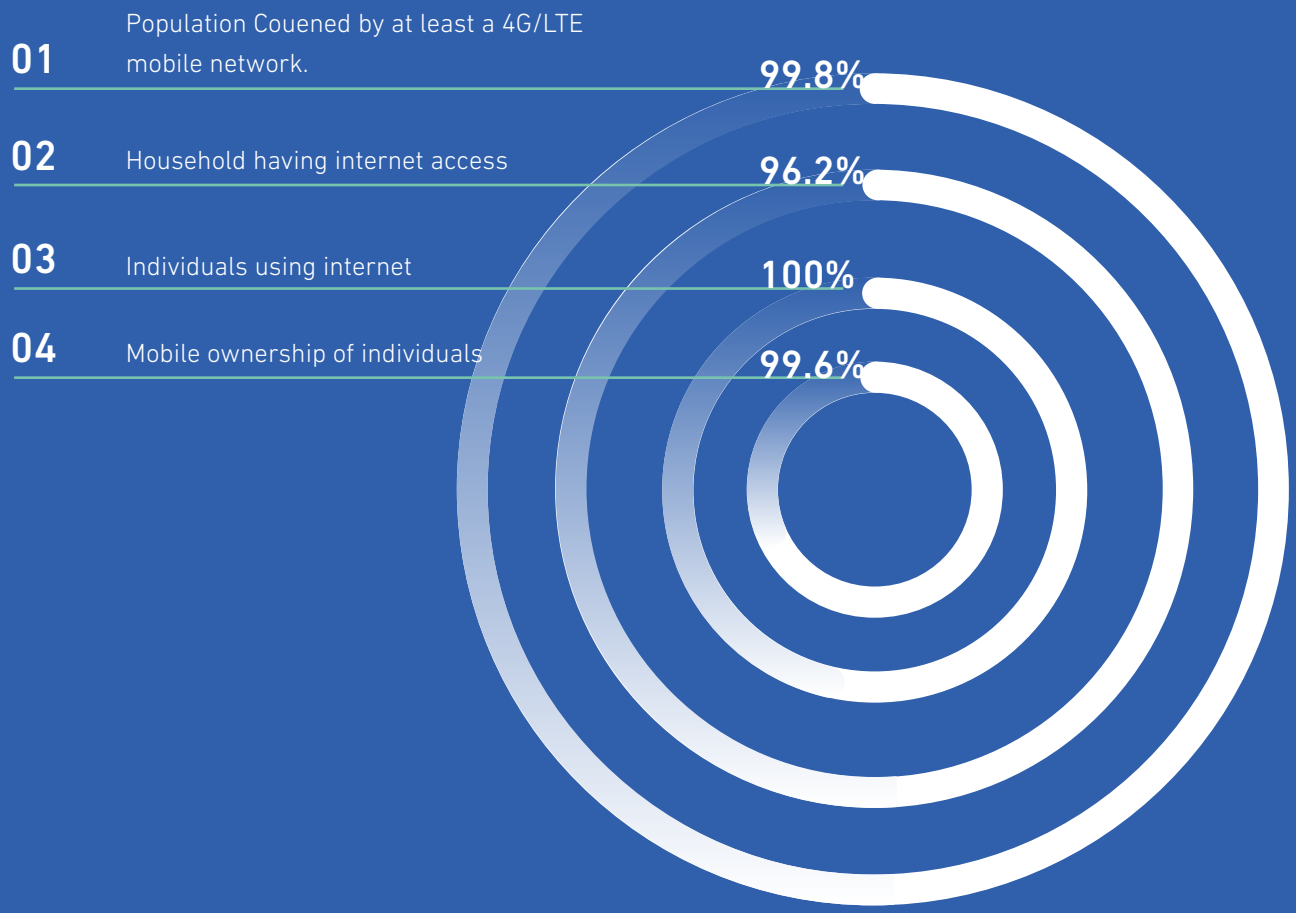


Figure 3 provides data to analyze Qatar's digital infrastructure and connectivity in 2022.

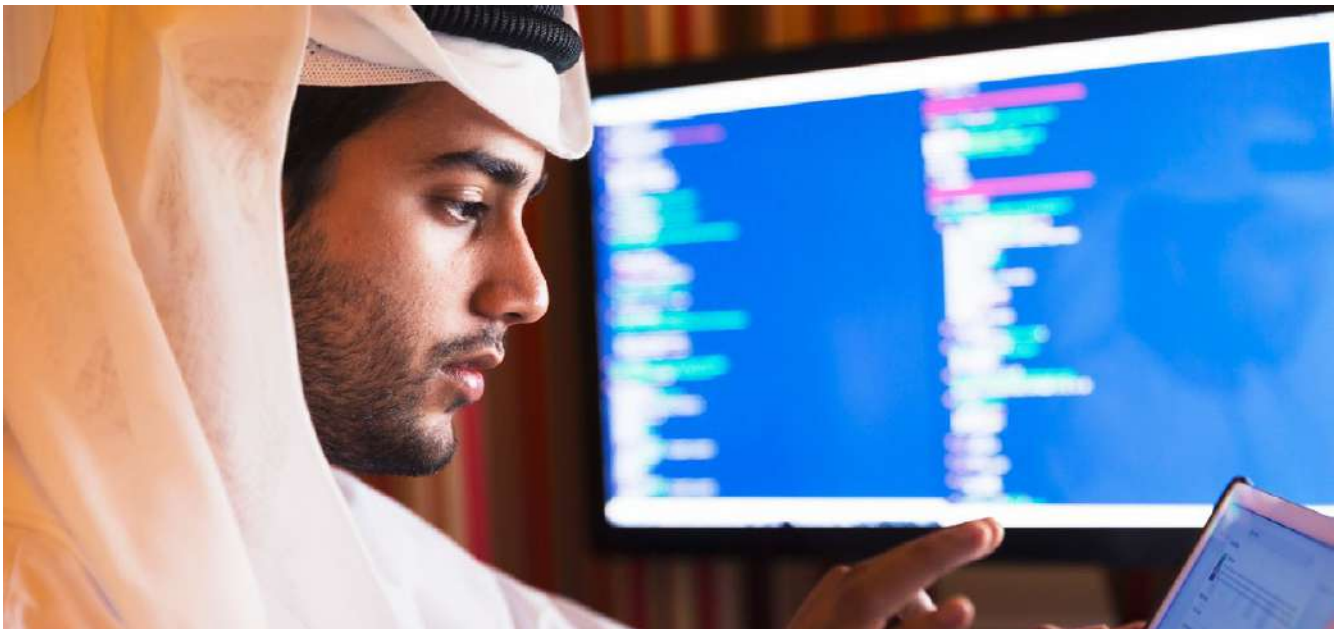
Digital Skills

To document Qatar'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.

The upper secondary education completion rate in Qatar was 83.49% in 2012. Gross tertiary education enrollment ratio stood at 35.09% in 2022, indicating moderate participation in higher education. The adult literacy rate was 98% in 2014. Government expenditure on education as a percentage of GDP was 1.87% in 2023.

The proportion of youth and adults with basic digital skills in Qatar showed moderate competency levels:

- 55.54% were able to copy or move a file or folder (2019).
- 21.21% had created electronic presentations with presentation software (2020).
- 37.12% could find, download, install and configure software (2020).



Digital Government

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

In terms of digital government services in 2022, Qatar had an operational government cloud platform in use. It had a government interoperability framework in draft or planned. It had an advisory/R&D government open-source software policy.

Qatar maintained both an open government portal and an open data portal. Regarding institutional frameworks for digital government in 2022, Qatar had established a government entity focused on government technology or digital transformation. It had established a government entity focused on public sector innovation. Qatar had institutionalized a whole-of-government approach to public sector digital transformation.

Finally, Qatar 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 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 Qatar 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

Qatar 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.

Conventions

Qatar 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 United nations office on drugs and crime - qatar supplementary agreement to establish the united nations regional centre for combating cybercrime in doha (cybersecurity)

04 League of arab states convention on combating information technology offences [third-party source] (cybersecurity)

05 Gulf cooperation council unified vat agreement (taxation)

06 Gulf cooperation council unified economic agreement (cross-cutting)

07 Gulf cooperation council common customs law (customs duties)

08 Gulf cooperation council agreement of the linking system for payment systems (electronic payments)
Berne convention for the protection of literary and artistic works (source code)

Guidelines, Recommendations, and Principles

Qatar 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. Qatar 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

Qatar has adopted or been influenced by the following model frameworks:

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

Other Commitments

01. Qatar 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, Qatar 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. Qatar 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)
06. ISO 31700-1:2023 (Consumer protection — Privacy by design for consumer goods and services) (Consumer protection)
07. ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity)
08. ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)
09. ISO 23195:2021 (Security objectives of information systems of third-party payment services) (Electronic payments)
10. ISO 32111:2023 (Transaction assurance in E-commerce — Principles and framework) (Electronic transactions)

Fora

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

01 United Nations Global Digital Compact (Cross-cutting)

02 Arab Federation for Digital Economy (Cross-cutting)

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

@dcorg | www.dco.org