



The Kingdom of Bahrain

Digital Trade Acceleration Initiative

Country Report

Disclaimer

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

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

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

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

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

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

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

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

© Digital Cooperation Organization 2025.
All rights reserved.

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

How to Read This Report

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

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

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

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

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

Table of Contents

01	Domestic Regulatory Environment Assessment	6
	Data Protection	8
	Cross-Border Data Transfers	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	49
	Size and Activities of the Digital Economy	50
	Digital Infrastructure and Connectivity	51
	Digital Skills	52
	Digital Government	53
03	International Commitments and Collaboration	54
	Commitments	56
	Fora	58

EXECUTIVE SUMMARY

The purpose of this report is to provide a detailed description of the regulatory environment affecting businesses and consumers engaging in digital trade.

We illuminate the regulatory environment from three perspectives:

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

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

Data Protection:

The data protection law requires the data subject's consent for data processing, providing alternatives. Data subjects are granted the rights to information, access, rectification, deletion, and consent withdrawal. Data processors are required to appoint a data protection guardian, establish local representation, and register with the government.

Cross-Border Data Transfers:

Data transfers are allowed to recipient countries with an adequate level of protection, designated by the government. Alternatively, transfers are allowed through case-based approval from the authority.

Location of Computing Facilities:

Bahrain does not require any form of data localisation. On the contrary, Bahrain subjects data stored in local data centres to the level of protection provided by the transferor's home country, for designated countries.

Online Consumer Protection:

Misrepresentations, failure to deliver after charging consumers, and charging consumers without authorisation are prohibited. The sending of unsolicited messages (spam) is not generally prohibited, as long as it does not cause disturbance to consumers. Data subjects have a right to object to direct marketing.

Electronic Transactions:

Electronic records carry the same evidential weight as written documents and can not be denied legal effect, validity, or enforceability based on their electronic form, with certain exceptions. The framework distinguishes between electronic signatures and secure electronic signatures.

Trade Facilitation with Digital Means:

Bahrain provides trade administration documents in electronic form and enables electronic submissions. The single window system is operational and internationally aligned.

Cybersecurity:

Several cyber offences are criminalised, including unlawfully accessing systems, conducting unauthorised surveillance, and damaging systems. Specific cybersecurity rules apply to critical infrastructure providers, including incident notification by employees.

Artificial Intelligence:

There is no law dedicated to regulating AI. The government has published ethical guidelines on AI and started developing a roadmap for AI adoption and procurement. The development of an AI Strategy has been referenced in official documents.

Source Code:

Computer software can be protected by copyright and as a trade secret. Source code disclosure is not mandated.

Digital Economy Taxation and Customs Duties:

Digital services and products are not subject to customs duties but the standard value-added tax rate applies. E-commerce imports are subject to customs duties as well as value-added tax. There is no specific direct tax targeting digital providers.

Electronic Payments:

Digital payments are governed by the general payment regulation framework under the oversight of the central bank. Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply.

SMEs and Digital Inclusion:

Bahrain has implemented a range of initiatives to support SMEs with a few related directly to the digital economy. These initiatives aim to enhance SMEs' access to digital technologies, e-commerce platforms, and international markets.



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.

Bahrain's data protection law requires the data subject's consent for data processing, providing exceptions such as the performance of a contract with the data subject, legal obligations, or the legitimate interest of the data controller. Data subjects are granted the rights to information, access, rectification, deletion, and consent withdrawal.

Data processors are required to appoint a "data protection guardian", establish local representation, and register with the government. The Personal Data Protection Authority is in charge of oversight.

Summary

- The comprehensive Personal Data Protection Law came into effect in August 2019. It governs the processing of data through fully or partially automated means as well as non-automated means.

Law requires the data subject's consent for data processing; with exceptions such as fulfilling a contract with the data subject, complying with legal or judicial obligations, protecting the vital interests of the data subject, or pursuing the legitimate interests of the data controller, provided that these do not infringe upon the fundamental rights and freedoms legally guaranteed to the data subject.

Data subjects are granted rights to:

- 01 information, access, rectification, erasure, and withdrawal of consent. Data controllers are required to appoint a "Data Protection Guardian" and designate an authorized representative for any individual or entity that does not habitually reside or have a place of business in the Kingdom but processes data using means within Bahrain, and register with the Authority.
- 02 The Personal Data Protection Authority is the entity responsible for supervision, oversight, and licensing of Data Protection Guardians.
- 03 The Law established the Personal Data Protection Authority (PDPA) to oversee the protection of individuals' rights and their personal data. The PDPA is also responsible for supervising data controllers and setting mechanisms, regulations, and standards for processing personal data, ensuring accuracy, security, reliability, complete privacy, and regular updates.

- **The PDPA serves as the primary authority responsible for ensuring the protection of personal data in Bahrain. Its key responsibilities include:**

- 01 Reviewing and recommending amendments to related legislation to align with internationally recognized standards.
- 02 Providing opinions on draft laws concerning personal data protection.
- 03 Representing Bahrain in international forums and collaborating with counterpart authorities on matters of shared interest. As an independent financial and administrative entity, the PDPA regulates rights and obligations, ensures compliance, issues licenses, and monitors data controllers' adherence to the law and its regulations. It also oversees the activities of Data Protection Guardians.
- 04 The PDPA is currently focused on developing the technical, legal, and procedural frameworks necessary to enforce the law across the public and private sectors. Its efforts are supported by other relevant authorities, ensuring comprehensive implementation and compliance.

Other authorities also collaborate regarding data protection:

- 01 The Information and eGovernment Authority regulates the governance of data-related sectors, ensuring that personal rights of citizens are protected. It promotes enhanced interactions between citizens and corporations with the government. It further plans to enhance the regulatory framework to strengthen data protection and build consumer confidence as part of the ICT Sector Strategy. It issued the ICT Sector Strategy and Digital Economy for 2022-2026.
- 02 The National Cybersecurity Center focuses on cybersecurity and addresses data protection, particularly in the context of personal data security on social media platforms. The NCSC has developed awareness materials aimed at educating the public on safeguarding personal information while engaging with social media.
- 01 The Telecommunications Regulatory Authority, responsible for the telecommunication sector, has issued guidance on privacy and data protection in telecommunications.

In 2022, Bahrain issued several executive orders to implement the provisions of the law. These include:

- 01 Defining technical and organizational measures necessary to safeguard personal data.
- 02 Establishing rules and mechanisms for international data transfers.

- 03 Regulating the role and responsibilities of Data Protection Guardians.
- 04 Setting fees for registration and renewal.
- 05 Outlining the rights of data subjects.
- 06 Establishing procedures for notifications, prior authorizations, and complaints.
- 07 Regulating the processing of sensitive personal data.
- 08 Prescribing safeguards for maintaining the confidentiality of data related to criminal cases and court rulings.
- 09 Setting conditions for creating public records of personal data accessible to the public.

The government has also issued policies focused on cloud migration and data protection:

The Backup Policy, established in 2023, mandates all government entities to implement secure and reliable backup solutions for mission-critical systems, including on-premises and cloud environments. The policy outlines requirements for planning, execution, testing, and validation of backups, with a 3-2-1 strategy, which involves maintaining three copies of data, storing two copies on different media, and keeping one copy offsite, with security controls defined by the National Cybersecurity Center.

- 01 Regulating the role and responsibilities of Data Protection Guardians.
- 02 Setting fees for registration and renewal.
- 03 Outlining the rights of data subjects.
- 04 Establishing procedures for notifications, prior authorizations, and complaints.
- 05 Regulating the processing of sensitive personal data.
- 06 Prescribing safeguards for maintaining the confidentiality of data related to criminal cases and court rulings.
- 07 Setting conditions for creating public records of personal data accessible to the public.

○ **The government has also issued policies focused on cloud migration and data protection:**

The Backup Policy, established in 2023, mandates all government entities to implement secure and reliable backup solutions for mission-critical systems, including on-premises and cloud environments. The policy outlines requirements for planning, execution, testing, and validation of backups, with a 3-2-1 strategy, which involves maintaining three copies of data, storing two copies on different media, and keeping one copy offsite, with security controls defined by the National Cybersecurity Center.



SOURCES

Primary Legislation

- Law No. (30) of 2018 Protection of Personal Data

Secondary Legislation

- Decree No. (78) of 2019 to Establish Personal Data Protection Authority
- Decision No. (43) of 2022 Regulating Standards of Data Protection
- Decision No. (44) of 2022 Regulating the Use of Personal Data
- Decision No. (45) of 2022 Regulating the Processing of Personal Data especially Sensitive and Confidential Data
- Decision No. (46) of 2022 Regulating Internal and External Audit of Personal Data
- Decision No. (47) of 2022 Regulating Fees related to Data Protection and Exemption Conditions
- Decision No. (48) of 2022 Rights of the Personal Data Subject
- Decision No. (50) of 2022 Regulating Secrecy and Privacy of Personal Data especially in Court Cases
- Decision No. (51) of 2022 Personal Data Use in Public Records

Guidelines

- National Cyber Security Center: Privacy Concerns and Threats
- Telecommunications Regulatory Authority: Facial Recognition Requirements Document
- Telecommunications Regulatory Authority: Guidelines on the Privacy of Individuals and Data Protection in the Telecommunications Sector
- Government of Bahrain: Presentation on the Information and eGovernment Authority
- Government of Bahrain: Presentation on Creating a Cloud Nation
- Information and eGovernment Authority: ICT Sector Strategy and Digital Economy (2022-2026)
- Information and eGovernment Authority: Cloud First in eGovernment
- Information and eGovernment Authority: Bahrain Cloud Strategy
- Information and eGovernment Authority: Bahrain Cloud Guidelines
- Information and eGovernment Authority: Bahrain Cloud First Policy
- Information and eGovernment Authority: Bahrain Backup Policy

Oversight Authorities

- Personal Data Protection Authority
- Information and eGovernment Authority
- National Cyber Security Center



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.

Bahrain's data protection law differentiates cross-border data transfers from in-country transfers. Transfers are allowed to recipient countries with an adequate level of protection, designated by the government. Alternatively, transfers are allowed through case-based approval from the authority. There are no special conditions for specific types of data transfers.

Summary

- Bahrain's Personal Data Protection Law distinguishes between cross-border data transfers and the handling of data within the country. Cross-border data transfers are permitted without prior approval from the Authority if the recipient country is deemed to provide an adequate level of protection as outlined in a list issued by the Authority (the Authority identifies countries deemed to have sufficient levels of data protection through ministerial decisions.)
- For transfers to countries not listed by the Authority, prior authorization must be obtained from the Personal Data Protection Authority on a case-by-case basis. The Authority evaluates factors such as the type of data, the purpose of processing, relevant international agreements, and the legal and regulatory frameworks of the destination country.
- Requests for prior authorization must include detailed information about the data processor, the nature of the data, the purpose and duration of processing, the origin and destination of the transfer, and the protection measures implemented in the receiving country.

Prior authorization is also required in the following scenarios:

- 01 Transfers within regional or international group structures.
- 02 Transfers from a data controller in Bahrain to a data controller or third party located outside the countries or regions approved by the Authority.

The authorization request must include the following:

- 01 A copy of the contract governing the transfer, ensuring that the data processing is strictly limited to the purposes specified in the agreement.
 - 02 Confirmation that the data will not be retained longer than necessary for the purpose of the transfer.
 - 03 Assurance that the data is accurate and reliable.
 - 04 Additionally, all technical and organizational safeguards for data processing must be adhered to.
 - 05 Furthermore, data subjects must:
 - 06 Be informed of the purpose of the data processing.
 - 07 Be given access to their personal data.
 - 08 Have the ability to correct, update, restrict, or delete their personal data.
 - 09 These measures aim to ensure full compliance with data protection principles and to uphold the rights of data subjects.
- In addition, the Cloud Law subjects data stored in local clouds to the rules of the foreign jurisdiction in which the customer is domiciled (see section on data localisation).

SOURCES

Primary Legislation

- Law No. (30) of 2018 Protection of Personal Data
- Legislative Decree No. 56 of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties ('Cloud Law')

Secondary Legislation

- Decision (42) of 2022 Transfer of Personal Data outside Bahrain
- Decision No. (43) of 2022 Regulating Standards of Data Protection
- Decision No. (44) of 2022 Regulating the Use of Personal Data
- Decision No. (45) of 2022 Regulating the Processing of Personal Data especially Sensitive and Confidential Data
- Decision No. (46) of 2022 Regulating Internal and External Audit of Personal Data
- Decision No. (47) of 2022 Regulating Fees related to Data Protection and Exemption Conditions
- Decision No. (48) of 2022 Rights of the Personal Data Subject
- Decision No. (6) of 2020 Designating the Kingdom of Spain as a Foreign State in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (21) of 2022 amending the Schedule attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (38) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating

Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties

- Decision No. (39) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (55) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (49) of 2023 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties

Guidelines

- Personal Data Protection Authority: Bahrain PDPA Form Templates
- Personal Data Protection Authority: Adequacy List
- Information and eGovernment Authority: Bahrain Cloud Strategy
- Information and eGovernment Authority: Bahrain Cloud Guidelines
- Information and eGovernment Authority: Bahrain Cloud First Policy
- National Enterprise Architecture (NEA): Bahrain National Framework for Institutional Structures
- Government of Bahrain: Presentation on Secure Data Transfer



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

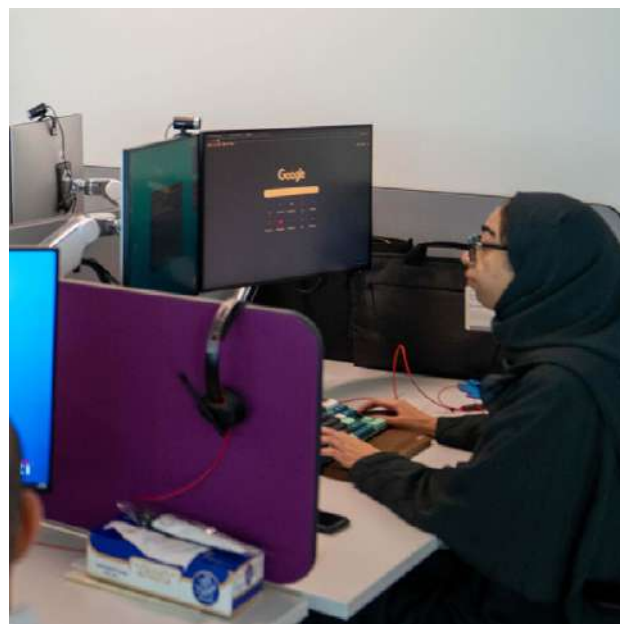
We analyse whether the framework generally requires data to be stored in the national territory. We then analyse whether data localisation requirements apply to specific data types, such as infrastructure or health data. For each identified localisation requirement, we distil the public policy objective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

Bahrain does not require any form of data localisation. On the contrary, the government emphasises the restrictions of such requirements on economies of scale and security, especially in cloud computing. To promote the local data storage market, the Cloud law subjects data stored in local data centres to the level of protection provided by the transferor's home country (for designated countries).

Summary

- Bahrain does not require any form of data localisation and instead prioritises cloud storage. The Backup Policy emphasises that cloud storage in a separate location is a suitable alternative to on-premise storage of backups. On the contrary, the Cloud Law encourages foreign investment in cloud computing services within its data centres by mandating that, for designated data centres and foreign countries, foreign consumers' data stored in Bahrain is subject to the data protection rules of the consumers' home country.
- The designated countries currently include Spain, the United Arab Emirates, Brazil, Israel, the United States of America, Switzerland, Egypt, the Republic of Maldives, the Sultanate of Oman, and Brunei Darussalam.
- Courts and authorities from these countries can issue binding judgments on disputes involving Bahraini service providers, including orders for data access, disclosure, and integrity maintenance.

Service providers then must notify the Bahraini Attorney General promptly upon receiving such orders from foreign authorities and provide a copy. Bahraini courts and the Attorney General can enforce final, non-appealable orders related to data access and integrity.



SOURCES

Primary Legislation

- Legislative Decree No. (56) of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties (“Cloud Law”)

Secondary Legislation

- Decision No. (6) of 2020 Designating the Kingdom of Spain as a Foreign State in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (21) of 2022 amending the Schedule attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (38) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of

Cloud Computing Services to Foreign Parties

- Decision No. (39) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (55) of 2022 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties
- Decision No. (49) of 2023 amending the Schedule Attached to Decision No. (67) of 2021 Designating Foreign States in Accordance with Legislative Decree No. (56) of 2018 regarding the Provision of Cloud Computing Services to Foreign Parties



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 consumer protection is governed by the general consumer protection framework, mainly the consumer protection law. The law prohibits misrepresentations, failure to deliver products or services after charging consumers, and charging consumers without authorisation. E-commerce platforms are not subjected to special obligations. Spam is not generally prohibited, as long as it does not cause disturbance to consumers. The data protection law further grants data subjects a right to object to direct marketing. Oversight is divided between the Consumer Protection Directorate under the Ministry of Industry and Commerce (retail products and services) and the Telecommunications Regulatory Authority (telecommunications and internet providers).

Summary

- The Consumer Protection Law, issued in 2012, covers all goods and services, including those ordered digitally, with exceptions for health and medical supplies as well as specific professions, including in the areas of law, engineering, medicine, accounting, and insurance.
- The Ministry of Industry and Commerce (MOIC) and the Telecommunications Regulatory Authority (TRA) have published various regulations and decrees on consumer protection. The Ministry issued a decree in 2014, which implements the Consumer Protection Law, and the Authority issued a decree in 2017, which regulates consumer protection in telecommunication services. Additional secondary legislation addresses regulating promotional campaigns, spam, and direct marketing, regulation of notifications sent by electronic means, and establishing an effective dispute settlement mechanism.

Multiple guidelines specify consumer protection rules:

- 01 The Economic Vision 2030 Framework commits to creating a legal and regulatory environment that ensures consumer protection and non-discriminatory treatment of businesses.
- 02 The Ministry of Transportation and Telecommunications' Sixth National Telecommunications Plan focuses on consumer transparency, digital accessibility, consumer rights, and raising consumer awareness.
- 03 The TRA's Work Plan aims to ensure fair treatment of all consumers, promote awareness, and manage dispute resolution and telecommunications regulation.
- 04 The Telecommunications Regulatory Authority also issued a guideline on consumer protection to be followed by telecommunications companies.

- 05 Spam is generally not prohibited unless it disrupts consumers. The Central Bank of Bahrain (CBB) Rule Book requires licensees to implement anti-spam and anti-spoofing measures to authenticate their mail servers and verify authorisation to send emails.

- In addition, the Data Protection Law provides data holders the right to object to direct marketing, including targeted advertising via text messages or email, and requires that entities cease such processing upon request from the data owner.

There are three main authorities overseeing consumer protection:

As of 2023, the Telecommunications Regulatory Authority (TRA), an independent governmental agency, is responsible for overseeing the consumer protection in the telecommunications sector. It addresses disputes, monitors compliance, and imposes fines. The last annual report by the Authority, for the year 2022, detailed their consumer protection efforts, including resolving 99% of the 2,740 complaints received.

- The Telecommunications Directorate, under the Ministry of Transportation and Telecommunications, issues regulations and suggests laws to ensure consumer protection.
- Finally, the Consumer Protection Department at the Ministry of Industry and Commerce acts as a mediator in complaints related to disputes within the commercial sector. The Consumer Protection Directorate is empowered to take action against online shopping violations committed by retailers that possess active Bahraini Commercial Registrations and operate within the Kingdom.
- The Kingdom of Bahrain is currently assessing digital trade related laws, including on consumer protection, and evaluating whether to formulate a digital trade law.

SOURCES

Primary Legislation

- Law No. (35) of 2012 with respect to Consumer Protection
- Legislative Decree No. (48) of 2002 Promulgating the Telecommunications Law
- Legislative Decree No. (38) of 2017 amending Legislative Decree No. 48 of 2002 of the Telecommunications Law
- Legislative Decree No. (18) of 2023 amending some provisions of the Telecommunications Law
- Law No. (30) of 2018 Protection of Personal Data

Secondary Legislation

- Minister of Industry and Commerce: Decision No. (66) of 2014 promulgating the Implementing Regulation of Law No. (35) of 2012 regarding Consumer Protection
- Minister of Industry and Commerce: Decision No. (113) of 2021 regarding the Regulation of Notification by Electronic Means
- Telecommunications Regulatory Authority: Decision No (3) of 2018 Promulgating the Regulation regarding Consumer Protection Disputes Settlement Mechanism
- Telecommunications Regulatory Authority: Decision No. (17) of 2017 promulgating the Regulation regarding Protection of Consumers of Telecommunications Services
- Prime Minister Edict No. (102) of 2023 for adoption of the Sixth National Telecommunications Plan
- Ministry of Industry and Commerce: Decision No. (1) of 1993 with regards to Promotional Campaigns
- Ministry of Industry and Commerce: Decision No. (109) of 2015 on prohibiting the imposition of additional amounts on the consumer when purchasing products with a Credit Card

Guidelines

- Telecommunications Regulatory Authority: Work Plan 2022-2023
- Telecommunications Regulatory Authority: Consultation report on Work Plan (2022-2023)
- Telecommunications Regulatory Authority: Consumer Protection Regulation
- Ministry of Industry and Commerce: Presentation of the Law No. (35) of 2012
- Ministry of Transportation and Telecommunications: Sixth National Telecommunications Plan
- Bahrain Economic Vision 2030
- Ministry of Transportation and Telecommunications: Telecommunications Plans 1 – 5

Oversight Authorities

- - Telecommunications Regulatory Authority
- - Ministry of Industry and Commerce
- - Ministry of Transportation and Telecommunications



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.

Bahrain has adopted a law on electronic communications and transactions, as well as a law on electronic transferable records. Electronic records carry the same evidential weight as written documents and cannot be denied legal effect, validity, or enforceability solely due to their electronic form. Exceptions include documents that must be notarised, such as real estate transactions and attorney powers, although the law mentions the possibility of developing an electronic notarisation system. The framework distinguishes between electronic signatures and secure electronic signatures, and foresees a mechanism for foreign accreditation. Finally, the government has laid the foundation for establishing a governmental authentication service and has accredited the first “trust service provider” who can accredit electronic authentication.

Summary

- The Law on Electronic Communications and Transactions, most recently amended in 2021, recognises electronic transactions as equivalent to paper-based transactions in civil and commercial contexts, provided they meet specified reliability criteria. These criteria include the method of generation, storage, communication, and signature, as well as the integrity and security of the electronic record. Exceptions include documents that must be notarised, such as real estate transactions and attorney powers, although the law mentions the possibility of developing an electronic notarisation system. In addition, the Electronic Transferable Records Law ensures that electronic records issued or used outside Bahrain retain legal validity (see section on paperless trade).

- The framework differentiates between electronic signatures and secure electronic signatures. An electronic signature is defined as data in electronic form that is attached to or logically associated with an electronic record, allowing for identification of the signatory and indicating their intent. "Secure" electronic signatures offer additional guarantees, being uniquely linked to the signatory, capable of identifying the signatory, and created using secure devices that ensure any alterations to the signed document are detectable.

- These signatures must be issued by an accredited service provider and are presumed legally binding if compliant with the law's requirements. Additionally, the framework allows foreign-issued electronic signatures to be recognised, provided the foreign trust service provider is accredited under Bahraini law.



- Electronic authentication is permitted in Bahrain, with the possibility of its application across all sectors, although specific regulations or restrictions may be determined by the Council of Ministers or the Minister of Justice in the future. The government may establish an electronic identification scheme, allowing for the secure management of digital identities for private transactions.
- The Telecommunications Regulatory Authority oversees the accreditation of trust service providers, including those operating outside Bahrain, to ensure compliance with national standards. As of 2021, the Authority issued its first accreditation to a private trust services provider, establishing a framework for digital identity management and secure electronic transactions within Bahrain. BENEFIT, as a Trust Services Provider (TSP), issues digital certificates for subscribers to digitally sign electronic cheques and offers three trust services.

- In 2021, the Telecommunications Regulatory Authority issued two regulations with regards to trust service providers. The first one details the accreditation requirements and standards for trust service providers, and the second one sets the fees for application and accreditation.
- Finally, a decree issued in 2018 outlines the technical requirements for the electronic transmission, reception, and updating of records and signatures that government agencies must follow, both within Bahrain and from abroad. It mandates the use of reliable electronic systems, standardised character encoding, and secure methods for electronic transactions between public entities and with individuals.
- It requires public entities to use certified digital certificates, trusted communication protocols, and comply with data protection laws. The decision emphasises secure electronic dealings, proper certification, and the application of precautionary measures to ensure the confidentiality and integrity of official electronic communications.



- The Kingdom of Bahrain is currently assessing digital trade related laws, including on data protection electronic communications and transactions, and evaluating whether to formulate a digital trade law. The government is also working on laws regarding e-bill of lading and electronic transferable records. Finally, a digital economy strategy is also currently being deliberated.

SOURCES

Primary Legislation

- Law No. (13) of 2006 amending some provisions of Decree-Law No. (28) of 2002 on electronic transactions
- Law No. (6) of 2012 amending Paragraph (d) of Clause (2) of Article (2) of Legislative Decree No. (28) of 2002 regarding Electronic Transactions
- Law No. (34) of 2017 amending Some Provisions of Legislative Decree No. (28) of 2002 regarding Electronic Transactions
- Legislative Decree No. (54) of 2018 promulgating the Law on Electronic Communications and Transactions repealing the previous Law No. 28/2002
- Law No. (29) of 2021 Amending Clause (d) of Article (23) of the Electronic Communications and Transactions Law promulgated by Legislative Decree No. (54) of 2018
- Legislative Decree No. (55) of 2018 with respect to Electronic Transferable Records
- Legislative Decree No. (28) of 2002 on electronic transactions [repealed]

Secondary Legislation

- Decree No. (45) of 2021 designating the Competent Administrative Authority of the Electronic Communications and Transactions Law promulgated by Legislative Decree No. (54) of 2018
- Decree No. (60) of 2022 nominating the competent administrative authority stipulated in Law No. (55) of 2018 on transferable electronic records
- Resolution No. (4) of 2021 Regulation on the Requirements and Standards for the Accreditation of Trust Services

- Resolution No. (5) of 2021 Determination of Fee Categories for Accreditation of Trust Service Providers
- Decision No. (36) of 2018 regulating the Technical Requirements for Sending, Receiving and Updating Electronic Records and Signatures of Public Entities
- Decision No. (74) of 2022 regarding the Linkage Service to the Commercial Records Electronic System

Guidelines

- Telecommunications Regulatory Authority issues the first licence to execute trust and e-signature services to BENEFIT company
- Benefit: Certification Authority
- Government of Bahrain: Presentation on E-Transactions

Oversight Authorities

- Telecommunications Regulatory Authority



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.

Bahrain's Customs Affairs website provides trade administration documents in electronic form, including in English, and enables electronic submissions. The single window system (Ofoq) is operational and aligned with other Gulf Cooperation Council members. E-commerce imports are subject to customs procedures for personal imports and must undergo the Ofoq customs clearance system if their value exceeds BHD 300 or they include restricted goods. Finally, simplified customs procedures apply to shipments valued below BHD 300.

Summary

- Bahrain has established a strong legal framework to support paperless trade, focusing on customs procedures and electronic documentation.

The 2018 Law on Electronic Transferable Records, aligned with the UNCITRAL MLETR, supports paperless trade by providing a framework for managing electronic transferable records. The law defines key terms, sets reliability standards, and ensures electronic records hold the same legal validity as paper documents. It supports replacing paper documents with electronic ones and vice-versa without altering legal obligations. The law also includes non-discrimination clauses for electronic records issued or used outside Bahrain and outlines the accreditation process for operators. In addition, the Electronic Communications and Transactions Law allows foreign trust service providers without a local presence to apply for accreditation (see section on electronic transactions).

- In 2006, Bahrain joined the Gulf Cooperation Council (GCC) Customs Union, adopting the 2019 unified guides for customs procedures at the first point of entry, which allow for online submission of customs documents and information. Importers, their representatives, or authorised customs brokers can generally submit documents electronically. GCC member states may, however, require original documents before or after the release of goods, as needed by the customs office.

Bahrain's secondary legislation includes bylaws for a unified customs system within the GCC, fee regulations for customs services, and resolutions



- defining customs brokers' roles and responsibilities. These regulations ensure transparency and standardisation in customs operations. In 2022, Bahrain amended the GCC Customs Union Convention to specify exemptions, risk management procedures, and administrative regulations.
- Guidelines for cross-border paperless trade include the Bahrain Customs Strategy (2024-2027) and the Organisational Fairness Questionnaire initiatives, which streamline trade documentation processes. Furthermore, the GCC guide allows forwarding agents to submit manifests in either paper or electronic format, with electronic forms being administratively sufficient in Bahrain. Importers and customs brokers can complete customs/import declarations electronically, and the customs office can process electronic submissions of accompanying documents and information.

○ Bahrain's Ofoq system, launched in 2011, serves as the electronic Single Window for trade documentation. It integrates several regulatory entities into a unified trade window, automates customs procedures, and supports the submission of electronic customs declarations, manifest management, and secure e-payments. The system aligns with international standards and facilitates cross-border trade through electronic data exchange. Furthermore, the Sijilat system, a one-stop-shop for business licensing, is a priority in view of digital transformation and will be enhanced through AI integration and increased scalability.

○ Additionally, Bahrain has a duty and tax de minimis threshold of BHD 300 for imports. Low-value shipments, particularly those handled by express couriers and postal services, do benefit from simplified customs procedures. For parcels exceeding BHD 300 or containing restricted goods, a simplified customs declaration is required through the Ofoq system.



○ Bahrain, the first state to enact the UNCITRAL's MLETR, also adheres to the Amended Kyoto Convention, the WTO Agreements on trade facilitation, and the League of Arab State Agreement to facilitate trade among Arab countries.

¹ The information on de minimis thresholds was retrieved from the Global Express Association.

SOURCES

Primary Legislation

- Law No. (1) of 2010 ratifying the free trade agreement between the countries of the Cooperation Council for the Arab States of the Gulf and the Republic of Singapore.
- Law No. (7) of 2012 on the establishment of a free trade area between the member states of the Cooperation Council for the Arab States of the Gulf and the countries of the European Free Trade Association (EFTA).
- Legislative Decree No. (10) of 2002 to approve the Unified System “Law” of Customs for the GCC, and to repeal the Customs Law of 1950
- Law No. (1) of 2006 to approve the establishment of the GCC Customs Union
- Legislative Decree No. (55) of 2018 with respect to Electronic Transferable Records
- Legislative Decree No. (45) of 2022 approving the amendment of some provisions of the unified system (law) of customs for the countries of the Cooperation Council for the Arab States of the Gulf
- Legislative Decree No. (10) of 2002 with respect to the approval of a unified customs law for Gulf Cooperation Council states [third party source]

Secondary Legislation

- Decision No. (3) of 2003 to issue the Bylaws of the Unified System “Law” of Customs for the GCC
- Decision No. (80) of 2017 regarding customs service fees
- Decision No. (16) of 2003 on the system of customs brokers
- Decision No. (8) of 2016 on the restructuring of the Parcel Opening and Inspection Committee
- Decision No. (7) of 2018 on the documents to be attached with the customs data and the information that must be included in these documents and the conditions that must be followed in this regard

Guidelines

- Presentation of Bahrain Customs Strategy 2024-2027
- Presentation on Creating User Account for Ofoq
- Bahrain Customs Strategy Roadmap
- Bahrain Customs Strategy Handbook
- Bahrain Customs: Authority Presentation on Online Shopping
- Bahrain Customs: Commercial Import Forms
- Bahrain Customs: Commercial Export Forms
- Bahrain Customs: Overview of Laws and Regulations
- Bahrain Customs: Single Window
- Bahrain Customs: GCC Unified Guide for Customs Procedures
- GCC Common Customs Law: Rules of Implementation and Explanatory Notes [other government source]



Cybersecurity

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

Guiding Questions

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

The Law No. (60) of 2014 concerning Information Technology Crimes criminalises several cyber offences, including unlawfully accessing systems, conducting unauthorised surveillance, and damaging systems. Penalties for violations are based on severity and the Public Prosecution can require providers to store and disclose data related to cyber offences. The National Cybersecurity Center is also responsible for oversight. In addition, specific cybersecurity rules apply to critical infrastructure providers, including incident notification by employees.

Summary

- The Law No. (60) of 2014 concerning Information Technology Crimes sets the punitive measures for data breaches, illegal content, and other information technology related crimes. The Law differentiates between crimes against IT systems, crimes related to IT means and crimes related to content.
- Two authorities are responsible for overseeing cybersecurity: The National Cybersecurity Center (NCSC) and the General Directorate of Anti-Corruption and Economic and Electronic Security (ACEES).
- The NCSC is the entity specifically mandated with the oversight of Law No. (30) of 2018 with Respect to Personal Data Protection. It further develops and implements Bahrain's National Cybersecurity Strategy, oversees the cybersecurity of critical national infrastructure sectors (setting technical standards and ensuring compliance), and facilitates information sharing and coordinates responses to national-level cyber threats. It further manages a national platform for monitoring cyber incidents and regulates information sharing among critical sectors. Finally, it promotes cybersecurity awareness and training, adopts cybersecurity indicators, and regularly publishes "cyber threat advisories" with guidance.
- The ACEES investigates cybercrimes, including hacking and online fraud, collaborating with law enforcement to gather evidence and prosecute offenders.

The NCSC issued the National Cybersecurity Strategy and the Critical National Infrastructure (CNI) Cybersecurity Controls. The National
- Cybersecurity Strategy focuses on protecting CNI, defined as vital assets essential for daily life whose loss or compromise could result in severe consequences and cause economic or social disruption. Identified CNI sectors include gas, electricity and oil, financial services, ICT, healthcare, government services, critical industry, and transportation.
- The CNI Cybersecurity Controls create sector-specific standards. Sector-specific cybersecurity controls have been developed for government, healthcare, financial, industrial, telecommunications, and transportation sectors, each addressing governance, defence, incident management, and audit to safeguard against cyber threats and enhance overall cybersecurity. The NCSC further issued guidelines on security threats, and best practices. Finally, the National Cybersecurity Strategy for 2025-2028 is being finalised and currently undergoing stakeholder feedback.
- Additionally, the Telecommunications Regulatory Authority issued a regulation on risk management in basic telecommunications infrastructure. Finally, the Central Bank of Bahrain has implemented comprehensive cybersecurity frameworks for financial institutions under its supervision. These frameworks include detailed guidelines on cyber risk management, incident reporting, and the establishment of robust cybersecurity controls.
- The Kingdom of Bahrain is currently assessing digital trade related laws, including on cybersecurity and data protection, and evaluating whether to formulate a digital trade law and a cybersecurity law.

SOURCES

Primary Legislation

- Law No. (60) of 2014 concerning Information Technology Crimes
- Law No. (2) of 2017, Bahrain ratifies the Arab Convention on Combating Information Technology Crimes
- Decree No. (65) of 2020 Establishing the National Cybersecurity Center

Guidelines

- National Cyber Security Center: National Cybersecurity Strategy
- National Cyber Security: CNI Cybersecurity Controls
- National Cyber Security: CyberWiser
- Telecommunications Regulatory Authority: Regulation for the Risk Management of Basic Telecommunications Infrastructure
- National Cyber Security Center: National Cybersecurity Risk Management Framework Presentation
- National Cyber Security Center: National Cybersecurity Risk Management Framework
- National Cyber Security Center: Cyber Trust Programme
- National Cyber Security Center: Templates of Cybersecurity Policies
- National Cyber Security Center: Baseline Cybersecurity Controls
- National Cyber Security Center: Cyber Essentials for Professionals

- National Cyber Security Center: Network & Enterprise Security
- National Cybersecurity Incident Response Team (CSIRT): Cyber Threat Advisories
- National Level Standard on Financial Cybersecurity Controls
- National Cyber Security Center: Financial Cybersecurity Controls
- Central Bank of Bahrain: Cybersecurity Risk Management Module
- Central Bank of Bahrain: Cybersecurity Control Guidelines
- Government of Bahrain: Presentation on Cybersecurity

Oversight Authorities

- National Cyber Security Center
- General Directorate of Anti-Corruption and Economic and Electronic Security under the Ministry of Interior [source not working]



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.

Bahrain has not adopted a binding regulatory framework to govern AI. The government is reportedly deliberating a comprehensive law, including AI guardrails and oversight mechanisms. To date, the government has published ethical guidelines on AI and started developing a roadmap for AI adoption and procurement. No regulatory agencies have issued guidelines on how existing rules apply to AI providers.

Summary

- Bahrain does not currently have primary or secondary legislation specifically dedicated to AI. The government is currently discussing a Law on AI and the Ministry of Industry is developing a policy on AI usage, although both are not yet publicly available and in early stages. Furthermore, the Ministry of Transportation and Telecommunications' Sixth National Telecommunications Plan mentions the current development of an AI Strategy.

Reportedly, an AI law – which is not publicly available yet – was approved by Bahrain's Upper House of the National Assembly (Shura Council). The law is yet to be formally presented to Parliament for approval. The law aims to address the increasing integration of AI in various sectors and prevent potential misuse. The law criminalises specific offences, such as tampering with biometric data, programming unauthorised AI systems, and using AI for malicious purposes, including terrorism. It also requires licensing for the programming and development of AI systems. To this end, the law mandates the formation of a special AI unit responsible for enforcing regulations, managing licences, and issuing fines.

- Bahrain has developed ethical guidelines for AI usage, focusing on privacy, data protection, inclusivity, sustainability, transparency, and accountability. These guidelines aim to ensure responsible AI deployment while balancing innovation with ethical considerations. Furthermore, Bahrain has established institutions, such as the AI Academy, which collaborates with firms to enhance AI training and development in the country. Furthermore, the Central Bank of Bahrain's rulebook includes a digital financial advice module including rules on "robo advisory."
- Recently, Bahrain's Upper House of the National Assembly (Shura Council) issued several news items related to AI. For example, the Parliamentary Division attended a workshop focusing on AI in parliaments, legislative quality, and parliamentary

- diplomacy. In addition, the Shura Council Chairman met with multiple stakeholders highlighting the efforts in organising the third Bahrain International Conference on Data and AI. Finally, the Shura Council Chairman emphasised the importance of investing in AI technologies to achieve sustainable development goals during his speech at the 3rd International Conference of Data 'Future of Everything'.

- Finally, Bahrain actively participates in international discussions on AI governance:

In November 2019, Bahrain's Economic Development Board and Information and eGovernment Authority co-hosted a workshop with the World Economic Forum Centre for the Fourth Industrial Revolution. The multi-stakeholder workshop explored AI procurement guidelines for Bahrain's public sector and proposed a roadmap for AI adoption in Bahrain, including the creation of a national data strategy, the development of a data sharing framework, and the creation of an intellectual property knowledge hub.

- Bahrain has also participated in the second Global AI Summit in September 2022, under the theme "Artificial Intelligence for the Good of Humanity". The conference focused on eight areas: smart cities, capacity building, healthcare, transportation, energy, culture, environment, and economic mobility. During the summit, member states of the Digital Cooperation Organization adopted the Riyadh AI Call for Action Declaration.
- Finally, in October 2023, during the Bahrain International eGovernment Forum, experts revealed the AI Roadmap, which outlines the strategic use of AI technologies, identifying benefits, risks, and ethical implications. It prioritises AI use cases in the public sector and categorises them based on impact and feasibility. The roadmap further emphasises the need for governance, cybersecurity, and sector-specific AI applications in healthcare, banking, and industry, aiming to enhance Bahrain's AI capabilities and address associated risks across political, economic, technical, and social domains.

SOURCES

Primary Legislation

- Draft AI Legislation [not currently public online – referenced in third party sources]

Guidelines

- Bahrain AI Guidelines
- Bahrain AI Roadmap
- Bahrain International eGovernment Forum
- Bahrain AI in Procurement Guidelines
- Shura Council: Participating in a Workshop on AI at the University of Hull
- Shura Council: The Chairman affirms the support of the Legislative Branch for AI
- Shura Council: The Chairman highlights the importance of investing in AI
- Shura Council: Patronising the International Conference on AI in Bahrain



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 protects computer software, written in either source or machine language, as a form of literary work, including the exclusive rights to reproduce, distribute, modify, and display the code. An exception is foreseen for the creation of a single software backup copy. Additionally, source code can be protected as a trade secret if it is kept confidential and has commercial value. Bahrain does not mandate source code disclosure.

Summary

- Bahrain's intellectual property protection is governed by multiple laws, primarily the Law on the Protection of Authors' Rights and Attendants' Rights Law, issued in 2006 and last amended in 2014. The law protects computer programs as intellectual works, granting developers and innovators both intangible and financial rights over their software and technology-related products. Creators have exclusive control over the reproduction, distribution, adaptation, and public performance of their software, which also covers derivative works and extends to 70 years after the creator's death. The law allows for limited free use of software for educational purposes or legal proceedings, provided that the rights of the original creators are respected. Recent amendments clarified the roles of authorities in enforcing the protection of software and enhanced protections against digital piracy. Unauthorised reproduction, distribution, or modification of software and source code is met with strict penalties. In February 2024, a decree designated the Ministry of Information as responsible entity for copyright oversight.
- The legal holder of a computer software copy is allowed to make a single backup copy for use in case of loss, damage, or unsuitability of the original, without needing the author's permission or paying compensation. The holder may also create an extracted, adapted, altered, or translated copy into another language for compatibility with a specific computer, provided it is solely for their use. Both the original and additional copies must be destroyed when there is no longer a legal basis for possessing the original copy.



- Bahrain does not require the sharing of source code. The law on trade secrets protects confidential business information and prohibits sharing without proper authorisation from the entity having such entity. Individuals and entities are prohibited from disclosing information if the information is confidential, not publicly known, and not easily accessible; it has commercial value due to its confidentiality; and its confidentiality is maintained through effective measures by the legal holder. The law also grants the trade secrets owner the right to prevent others from violating the confidentiality through actions contrary to lawful commercial practices, and allows the owner or a licensed third party to share the trade secrets with or without consideration.
- Additional legislation includes the Manufacturing and Trading in Compact Discs Law, which addresses the protection of digital content, and the Design of Integrated Circuits Law, which focuses on the protection of semiconductor designs

SOURCES

Primary Legislation

- Law No. (7) of 2003 on Trade Secrets
- Law No. (35) of 2005 amending Article (5) of Law No. (7) of 2003 regarding Trade Secrets
- Law No. (5) of 2006 on Integrated Circuit Designs
- Law No. (12) of 2006 amending some provisions of Law No. (7) of 2003 on Trade Secrets
- Law No. (15) of 2006 on the Manufacture and Circulation of Compact Discs
- Law No. (22) of 2006 on the protection of Copyright and related rights
- Law No. (12) of 2008 amending Article (13) of Law No. (22) of 2006 on the protection of Copyright and related rights
- Law No. (3) of 2011 amending Certain Provisions of the Trademark Law and the Protection of Copyright and Related Rights
- Law No. (5) of 2014 amending some provisions of Law No. (22) of 2006 on the protection of copyright and related rights
- Law No. (6) of 2014 approving the law (system) of trademarks of the Cooperation Council for the Arab States of the Gulf

Secondary Legislation

- Decree No. (18) of 2024 naming the competent administrative authority and the competent minister applying the provisions of Law No. (22) of 2006 on the Protection of Copyright and Neighbouring Rights
- Resolution No. (65) of 2016 issuing the Executive Regulations of the GCC Trademark Law issued by Law No. (6) of 2014 and making it come into force [third party source]

Guidelines

- Government of Bahrain: Presentation on the Legal Framework of Intellectual Property Rights



Digital Economy Taxation and Customs Duties

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

Guiding Questions

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

Digital services and products are not subject to customs duties but the standard value-added tax rate applies. E-commerce imports are subject to customs duties, if they are imported from outside the Gulf Cooperation Council and exceed the de minimis threshold of BHD 250, as well as value-added tax. Tax registration is mandatory if the total value of supplies per year exceeds BHD 37,500 and can be done electronically.

Summary

- Taxation in Bahrain is primarily governed by the Value Added Tax (VAT) Law of 2018. The law stipulates that digital services and products are generally classified as services, making them subject to VAT unless an exemption or zero-rating applies. Most taxable supplies of goods and services, including digital services or products, are taxed under these general provisions. Since the introduction of VAT, Bahrain has issued three decree laws in 2017, 2018, and 2021 to refine the application and procedures related to VAT. The latest decree increased the standard VAT rate from 5% to 10% as of January 1, 2022.

The National Bureau for Revenue (NBR) is the primary authority responsible for overseeing and implementing VAT regulations in Bahrain. The Bureau published various guidelines on their website, including the Summary of Bahrain VAT Executive Regulations, and a list of basic food items exempt from VAT standard rate. These regulations aim to clarify VAT compliance and provide businesses and consumers with information on taxable and non-taxable items.

- Customs Affairs in Bahrain manages the import and export of goods and enforces compliance with customs regulations. Their website includes an FAQ section designed to assist importers, exporters, and visitors with inquiries about customs duties, restrictions, and required documentation. Additionally, a list of prohibited and restricted items is published to ensure adherence to Bahrain's customs laws.

- In alignment with Bahrain's commitment to trade facilitation, Customs Affairs has outlined its 2024-2027 Strategy, focusing on enhancing transparency and streamlining customs processes. The strategy aims to promote efficient trade practices while maintaining security and regulatory compliance in Bahrain's customs system.
- Bahrain is part of various international agreements governing customs and taxation, including the GCC VAT framework. The Kingdom has 45 double tax agreements with the following jurisdictions: Algeria, Austria, Bangladesh, Barbados, Belarus, Belgium, Bermuda, Bulgaria, Brunei, China, Czech Republic, Cyprus, Egypt, Estonia, France, Georgia, Hungary, Iran, Ireland, Isle of Man, Jordan, Lebanon, Luxembourg, Malaysia, Malta, Mexico, Morocco, Netherlands, Pakistan, Philippines, Portugal, Republic of Korea, Seychelles, Singapore, Sri Lanka, Sudan, Switzerland, Syria, Tajikistan, Thailand, Turkey, Turkmenistan, United Kingdom, Uzbekistan, Yemen.
- Bahrain has also signed and ratified the Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (MLI). The MLI entered into force for Bahrain on June 1, 2022.

SOURCES

Primary Legislation

- Law No. (39) for the year 2017 ratifying the Common Excise Tax Agreement of the States of the Gulf Cooperation Council
- Law No. (40) for the year 2017 regarding the Excise Tax
- Law No. (33) for the year 2021 to amend the VAT Law of 2018
- Legislative Decree No. (48) for the year 2018 regarding Value Added Tax

Secondary Legislation

- Decision No. (17) for the year 2017 issuing the Executive Regulations for the Law No. (40) for the year 2017 regarding Excise Tax
- Decision No. (31) for the year 2022 regarding amending some provisions of the Executive Regulations for the Law No. (40) for the year 2017 regarding Excise Tax issued by Decision No. (17) for the year 2017
- Decision No. (48) of 2018 specifying the scope of application of the Law No. (33) of 2021

Guidelines

- National Bureau for Revenue: Summary of the Bahrain VAT Executive Regulations
- National Bureau for Revenue: Summary of the Bahrain Excise Executive Regulations
- National Bureau for Revenue: Executive Regulations of the VAT in Bahrain
- Customs Affairs: Strategy
- Customs Affairs: Prohibited and Restricted Items
- Customs Affairs: Customs Affairs Individuals FAQ
- National Bureau for Revenue: Products not subject to VAT

International Frameworks

- The Unified Agreement for VAT of the Cooperation Council for the Arab States of the Gulf



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

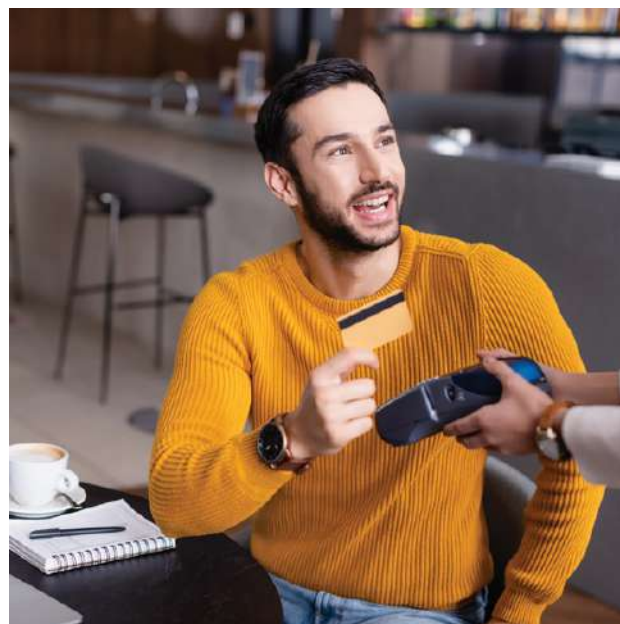
We outline whether there is a regulatory framework specifically addressing electronic payments. We then distil know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to electronic payments. In addition, we delineate licensing requirements and procedures for entities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

Digital payments are governed by the general payment regulation framework under the oversight of the central bank. The central bank's regulations and the Anti Money Laundering Law impose know-your-customer, anti-money-laundering, and counter-terrorism-financing rules, which apply to all bank licensees. For cross-border wire transfers, intermediaries and banks must retain originator and beneficiary information and adopt risk-based policies to prevent transfers that lack such information.

Summary

- The Central Bank of Bahrain (CBB) Law of 2006, which governs digital payments, has been amended several times to support the evolving financial sector. Key amendments include the 2015 update, which introduced credit information centres, emphasised data protection, privacy, and consumer rights, and imposed administrative penalties. The 2016 amendment expanded the CBB's services, introduced regulations on service fees, and enhanced financial protections for clients. In 2020, an amendment further strengthened the CBB's authority and imposed stricter regulations on financial institutions. In 2020, Bahrain also issued a law ratifying the Convention on the Payment Systems Linkage among the GCC Countries and a law ratifying the Agreement of Establishment and Articles of Association of the Gulf Payments Company. Finally, the Legislative Decree on the Prevention and Prohibition of Money Laundering establishes know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to digital payments.
- The Central Bank of Bahrain is the main authority for overseeing financial and payment systems, including banking, insurance, capital markets, and fintech activities. It has broad powers to regulate digital payments, electronic fund transfer systems (EFTS), and digital wallets. The Central Bank's regulatory sandbox allows licensed institutions and startups to test innovative financial technologies under its supervision, ensuring the safe implementation of digital payment solutions.

Bahrain issued a decree in 2006 following the law that establishes the central bank. The decree



- repeals previous legislation, including the 1973 decree that established the Bahrain Monetary Agency and the 1987 decree regarding insurance companies. It integrates various legal provisions to ensure that the CBB operates with broad regulatory powers over Bahrain's financial sector, including banking, insurance, and capital markets. Secondary legislation includes the Bahrain Open Banking Framework introduced in 2020, which enables third-party access to banking data via APIs, fostering the development of digital financial services. In 2021, the second phase of the framework was introduced to enhance the range, effectiveness, and cost-efficiency of financial services, with a focus on improving customer experience.
- The CBB Rulebook states that individuals or entities wishing to provide regulated banking services, which include deposit-taking and providing credit, must obtain a licence as a bank licensee from the CBB. Regulated banking services also encompass supplementary activities such as issuing or admin-

istering means of payment, including payment instruments and stored value like credit cards and electronic purses. Bank licensees involved in Account Information Services or Payment Initiation Services must adhere to the Open Banking Module requirements which also governs specialised licensees such as money changers, financing companies, trust service providers, and ancillary service providers. The CBB further issues a stand-alone licence for payment service providers. The CBB has also allowed the use of digital wallets to store essential user data, including payment and personal information, which can be utilised for credit or debit cards, loyalty cards, gift cards, coupons, hotel reservations, and more. Moreover, the CBB rulebook includes a module on crypto assets that was recently amended to enable digital token offerings. Finally, the CBB is focusing on SME participation in digital payments, as well as open banking.

The central bank has created a regulatory sandbox which is a virtual space designed for testing innovative financial solutions, providing CBB-licensed institutions, FinTechs, startups, and companies with the opportunity to evaluate the viability and effectiveness of their innovations in a live, controlled environment with volunteer participants. The central bank oversees and supervises the sandbox, regularly updating its regulations to keep pace with the evolving technologies and solutions being tested.

Furthermore, the central bank is currently working on developing a digital version of the Bahraini Dinar, designed to support peer-to-peer payments without intermediaries, mimicking cash while remaining intangible and virtual, and operating on



distributed ledger technology, a central addressing system aiming to simplify fund transfers by replacing long IBAN numbers with unique identifiers (such as national IDs or phone numbers).

In 2020, the GCC member countries implemented AFAQ, a regional payment system designed to provide a faster, more secure, and cost-effective method for transferring funds across borders. Operated by the Gulf Payments Company, AFAQ is a Real-Time Gross Settlement (RTGS) service that facilitates cross-border payments between GCC countries. This system aims to support the growth of trade and investment flows among GCC member states, thereby contributing to economic diversification within the region.

SOURCES

Primary Legislation

- Law No. (64) of 2006 promulgating the Central Bank of Bahrain and Financial Institutions Law
- Law No. (14) of 2020 amending some provisions of the Central Bank of Bahrain and Financial Institutions Law promulgated by Law No. (64) of 2006
- Law No. (6) of 2023 ratifying the Convention on the Payment Systems Linkage among the Countries of the Gulf Cooperation Council
- Law No. (9) of 2020 ratifying the Agreement of Establishment and Articles of Association of the Gulf Payments Company
- Legislative Decree No. (34) of 2015 amending some provisions of the Central Bank of Bahrain and Financial Institutions Law promulgated by Law No. (64) of 2006
- Legislative Decree No. (21) of 2016 amending some provisions of the Central Bank of Bahrain and Financial Institutions Law promulgated by Law No. (64) of 2006
- Legislative Decree No. (4) of 2001: Prevention and Prohibition of Money Laundering and Terrorism Finance

Secondary Legislation

- Decree No. (64) of 2006 with respect to promulgating the CBB and Financial Institutions Law
- Central Bank of Bahrain: Regulations and Resolutions
- Central Bank of Bahrain Rulebook

Guidelines

- Central Bank of Bahrain: General Requirements Module
- Central Bank of Bahrain Rulebook: Vol. 1 – Licensing Requirements Module
- Central Bank of Bahrain Rulebook: Vol. 5 – Specialised Licensees Module
- Central Bank of Bahrain: Presentation on Licensing and Registration
- Central Bank of Bahrain Licensing Directory
- Central Bank of Bahrain: Open Banking Module
- Central Bank of Bahrain: Users Guide Module
- Central Bank of Bahrain: Specialised Licensees
- Central Bank of Bahrain: Index Financial Crimes
- Central Bank of Bahrain: Financial Crimes Module
- Central Bank of Bahrain: FinHub 973 | Regulatory Sandbox
- Central Bank of Bahrain: Rulebook
- Central Bank of Bahrain: Bahrain Digital Payments Landscape

International Frameworks

- AFAQ - Gulf Payments
- GCC Net



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. Bahrain has implemented a range of initiatives to support SMEs with a few related directly to the digital economy. These initiatives aim to enhance SMEs' access to digital technologies, e-commerce platforms, and international markets. The government's approach includes regulatory measures, financial support, and capacity-building programmes tailored to the needs of small businesses.

Summary

○ The Ministry of Industry and Commerce launched and implemented the National eCommerce Strategy 2019-2022, which comprised 13 initiatives within the framework of the support provided by the Ministry to companies, SMEs and startups to foster digital trade. It focuses on developing regulatory policies, improving consumer confidence, and supporting SMEs.

○ KPIs included raising the number of eCommerce companies, increasing the number of women-led eCommerce businesses and multiplying the number of virtual CRs in the eCommerce field. In addition, recognizing the needs derived from the Strategy, the Ministry issued a resolution regarding virtual stores and a ministerial order regarding retail sale via internet activity for companies with foreign capital.

○ The Ministry of Industry and Commerce also leads the promotion of SMEs through the SME Development Board, established in 2017. This board coordinates efforts between several government entities and the private sector to strengthen SMEs' capacities and boost their competitiveness domestically, regionally, and globally.

○ The board's integrated task plan focuses on five strategic themes: access to finance, access to markets, streamlining the business environment, skill development, and fostering innovation.

As part of Bahrain's Economic Recovery Plan, the ministry has issued the SME Development Board Plan 2022-2026 (SDB 2.0). This plan outlines



○ strategic pillars and initiatives aimed at strengthening SMEs' capacities and boosting their competitiveness domestically, regionally, and globally. Specific digital initiatives within these pillars include export facilitation, the "Tijara" Platform for banking solutions, and support for innovation and technology transfer through the Bahrain Innovation and Technology Transfer Centre.

○ Export Bahrain, a government entity, offers export facilitation services to assist companies in leveraging e-commerce for international trade. Its services include online e-commerce training tutorials, multi-channel marketing support tools, and resources to increase exposure on e-commerce platforms. Export Bahrain also provides exclusive rates for building online stores, which include access to multi-currency payment gateways, web development, marketing, and shipping support.

- To enhance regional market access for SMEs, Export Bahrain has partnered with Talabat, a private food delivery organisation. This collaboration enables SME exporters to sell Bahraini-made products through Talabat's online platforms across the MENA region, expanding their digital reach.
- In the financial sector, the government-owned Bahrain Development Bank has launched 'Tijara', a digital banking service specifically targeted towards small businesses. This service aims to provide tailored solutions for SMEs to manage their business transactions and expand their access to affordable financing through digital channels.
- The Bahrain Technology Transfer Center, another initiative under the SME Development Board, focuses on improving productivity and stimulating growth for emerging and digital companies. The centre facilitates the transfer of technologies developed by academic staff to the private sector, securing intellectual property protection and expediting the commercialisation of innovations and products.



SOURCES

- Ministry of Commerce and Industry: eCommerce National Strategy
- Ministry of Commerce and Industry: SME Development Board
- Ministry of Commerce and Industry: SME Development Board 2.0
- Export Bahrain: E-Commerce Facilitation
- Export Bahrain: Strategic Agreement with talabat
- Bahrain Development Bank: Launch of 'tijara'



02

Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Bahrain'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 Bahrain'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 account for 10.73% of Bahrain's imports. The share of advanced technology products in exports was considerably lower at 2.12%, indicating a technology trade imbalance.

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

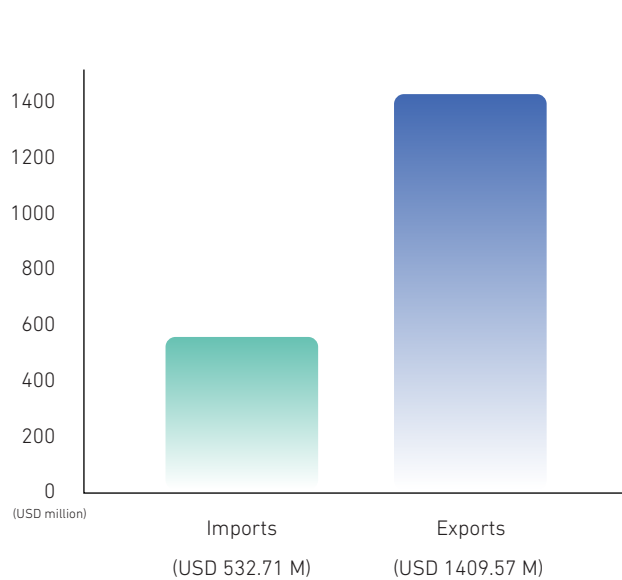


Figure 1 provides data for Bahrain's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

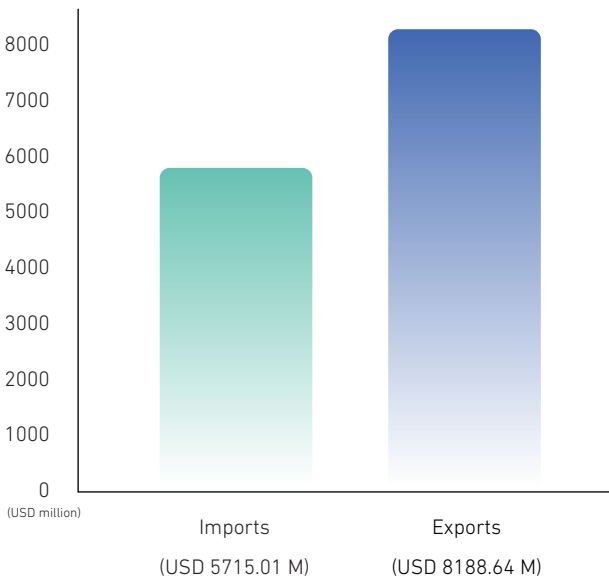


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Bahrain'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

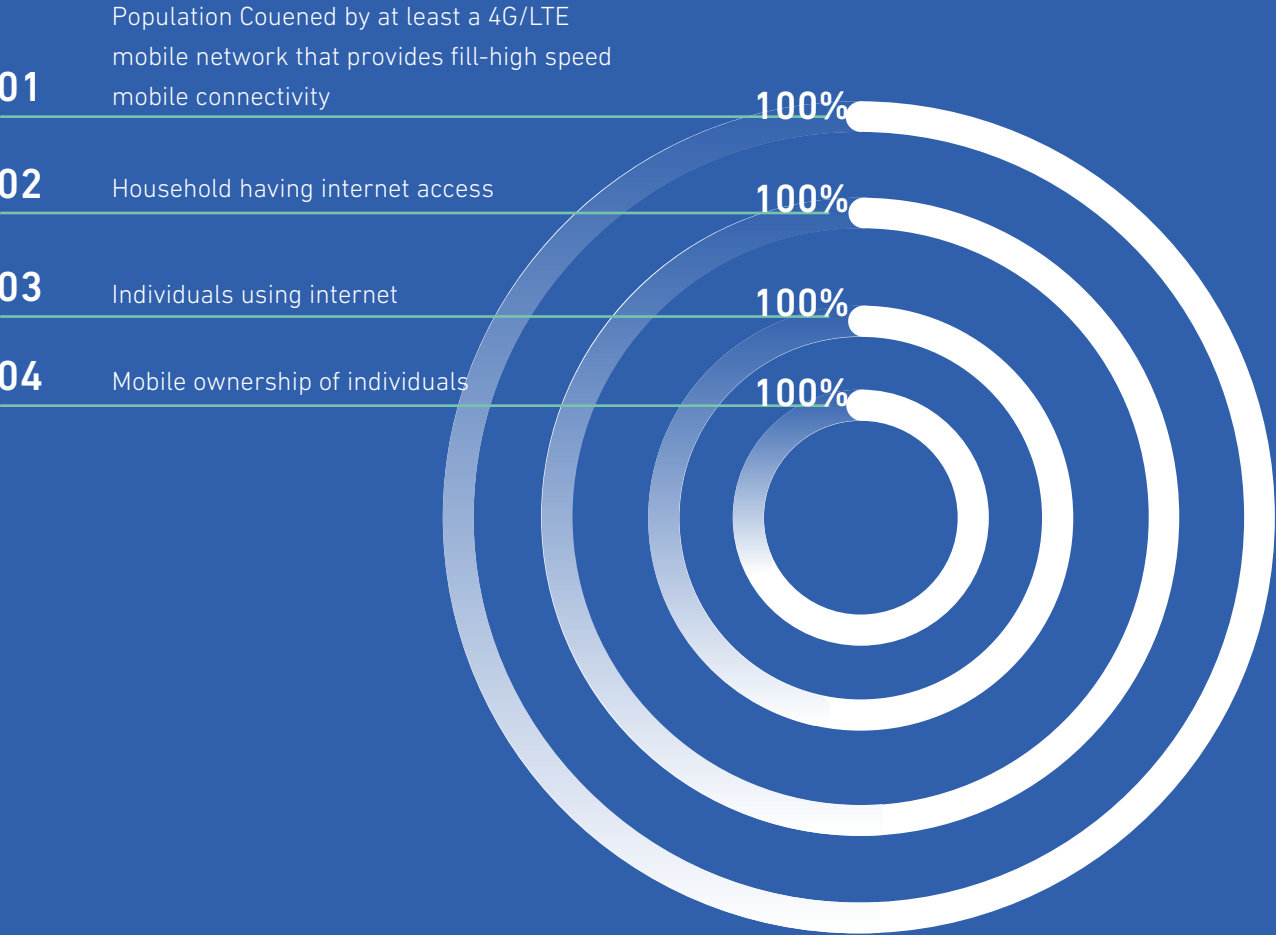


Figure 3 provides data to analyze Bahrain's digital infrastructure and connectivity in 2022.



Digital Skills

To document Bahrain'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 71.96% in 2023, indicating relatively high participation in higher education. The adult literacy rate was 98% in 2023, demonstrating near-universal basic literacy. Government expenditure on education as a percentage of GDP was 1.99% in 2022.

The proportion of youth and adults with basic digital skills in Bahrain showed relatively high competency levels:



71.12% were able to copy or move a file or folder (2019);



38.63% had created electronic presentations with presentation software (2021); and



65.16% could find, download, install and configure software (2021).



Digital Government

To examine the state of digital government in Bahrain, we rely on the [World Bank's GovTech dataset](#). In terms of digital government services in 2022, Bahrain had an operational government cloud platform in use and had implemented a government interoperability framework. It did not have a government open-source software policy or action plan. Bahrain maintained both an open government portal and an open data portal.

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

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

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

Bahrain 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. Bahrain has entered the [Bahrain - United States Free Trade Agreement](#) which contains provisions pertinent to Electronic Transactions and Customs Duties

Conventions

- 01 International Covenant on Civil and Political Rights (Data Protection)
- 02 United Nations Convention on the Use of Electronic Communications in International Contracts (Electronic Transactions)

- 03 G20/Organisation for Economic Co-operation and Development Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (Taxation)
- 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)
- 09 Berne Convention for the Protection of Literary and Artistic Works (Source Code)

Guidelines, Recommendations, and Principles

Bahrain 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)

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

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

Models

- 01 Bahrain 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)



Other Commitments

- 01 Bahrain 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, Bahrain 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 Bahrain 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

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

Fora

- 01 Bahrain 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)

