Digital Cooperation Organization

Kuwait

Digital Trade Acceleration Initiative

Country Report

Disclaimer

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

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

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

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

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

DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.
The use of this Document is solely at the User's own risk. Under no circumstances shall DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

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

How to Read This Report

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

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

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

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

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

Table of Contents

EXECUTIVE SUMMARY

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

01 A comprehensive regulatory assessment explains the regulatory environment across twelve policy areas.

02 A factsheet describes the local digital economy across four dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.

03 An overview of existing international commitments characterises efforts to accelerate digital trade.

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

Data Protection:
Data processing is only legitimate with data subjects' consent, with certain alternatives. Data subject rights include the right to information, access, correction, and deletion. Providers must appoint a data protection officer but are not required to register or establish local representation.

Cross-Border Data Transfers:
Kuwait recently repealed its Data Classification Policy, which is yet to be replaced. The Policy allowed only public data and private insensitive data to be transferred, albeit only with user consent. Location of Computing Facilities: Kuwait recently repealed its Data Classification Policy, which is yet to be replaced. The Policy required data localisation for private sensitive data and highly sensitive data.

Online Consumer Protection:
Online consumer protection is regulated under the general consumer protection law, which grants consumer rights to safety, quality, information, and fair redress rather than prohibiting practices. The sending of unsolicited messages (spam) is not generally prohibited, but allowed only during specific times and when accompanied by identifying information and an option to unsubscribe.

Electronic Transactions:
The law on electronic transactions recognises electronic records, documents, messages, transactions, and signatures as equivalent to written ones, with certain exceptions. Kuwait differentiates between electronic signatures and protected electronic signatures. Providers have access to an online portal for registration.

Trade Facilitation with Digital Means:

Kuwait provides trade administration documents for imports in electronic form and enables electronic submission, through the Kuwait General Administration of Customs (KGAC) portal. Kuwait is currently integrating various government agencies into a unified system, with the stated goal to achieve an Electronic Single Window.

Cybersecurity:

Certain online conduct, including unauthorised access to and theft of data, is criminalised. Notification is required when personal data of a "large number" of users is improperly disclosed, towards authorities and users.

Artificial Intelligence:

There is currently no binding framework devoted to the governance of AI. Kuwait is in the process of developing its framework for AI regulation, with current efforts focusing on establishing an AI authority.

Source Code:

Kuwait's copyright law provides protection for "computer programs", foreseeing exceptions for personal use and educational purposes. Kuwait does not generally mandate the sharing of source code. Access to source code can be required for critical applications in the banking sector, in public tenders, and in cybercrime investigations.

Digital Economy Taxation and Customs Duties:

Kuwait does not impose import-related fees or indirect taxes on digital services/products. Regarding e-commerce imports, Kuwait imposes a standard customs duty, but no indirect taxes. No direct tax specifically targets digital providers. Electronic Payments: Anti-money-laundering and counter-terrorism-financing requirements apply to electronic payment providers. Such providers must register with the central bank.

SMEs and Digital Inclusion:

While the government has established a general framework for SME development, evidence of direct digital economy support initiatives remains sparse. The primary mechanism for SME assistance is a national fund, which has begun to incorporate digital elements into its offerings.

Location of Computing Facilities:

Kuwait demands data localization for certain data types, based on its classification of data: Private sensitive data and highly sensitive data cannot be transferred internationally.

Electronic Payments:

Anti-money-laundering and counter-terrorism-financing requirements apply to electronic payment providers. Such providers must register with the central bank.

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.

Kuwait's data protection regime is not centralised but rather draws from several laws. Data collection and processing are only legitimate if data subjects consent, although alternatives such as legal obligations or the protection of data subjects' information are available. Data subject rights include the right to information, access, correction, and deletion. Providers must appoint a data protection officer but are not required to register or establish local representation. Data protection is overseen by several sectoral regulators, not a dedicated data protection agency.

Summary

- There is no comprehensive legislation on data protection in Kuwait. The Electronic Transactions Law addresses data protection in a dedicated chapter. The Exchange of Credit Information Law enforces the confidentiality of credit data and restricts its collection or sharing without consent, except where authorised by law. The Cybercrime Law imposes heavy penalties for the retrieval of personal data without permission (see cybersecurity section).

- There is no dedicated personal data protection agency. The Communication and Information Technology Regulatory Authority (CITRA) is responsible for data protection in the telecommunications and IT sectors.

- The CITRA is a public authority with an independent corporate body and financial independence, empowered to draft rules, enforce compliance, and impose penalties. Additionally, the Central Agency for Information Technology (CAIT), an independent government agency, executes these rules. Furthermore, the Central Bank of Kuwait (CBK), a public institution with an independent juristic personality, oversees data protection within regulated entities.

- The CBK issues regulations, supervises compliance, and imposes penalties to ensure data protection standards are maintained.

  Kuwait has implemented several regulations related to data protection. The Executive Regulation of the Electronic Transactions Law provides detailed guidelines for its implementation, ensuring secure and efficient electronic transactions.

- Similarly, the Executive Regulation of the Exchange of Credit Information Law offers comprehensive guidelines for its implementation, focusing on the secure exchange of credit information.

- Additionally, the Data Privacy Protection Regulation by CITRA sets guidelines for protecting personal data collected by telecommunications and IT service providers, whether within or outside Kuwait.

- The Cyber Security Framework by the Central Bank of Kuwait (CBK) imposes data protection obligations on all entities supervised by the CBK, ensuring robust cybersecurity measures are in place.

SOURCES

Primary Legislation

- Law No. 20 of 2014 Concerning Electronic Transactions
- Law No. 63 of 2015 Concerning Combating Cyber Crimes
- Law No. 9 of 2019 Regulating The Exchange of Credit Information

Secondary Legislation

- Communication and Information Technology Regulatory Authority: Data Privacy Protection Regulation
- Central Bank of Kuwait: Cyber Security Framework for the Kuwaiti Banking Sector
- Executive Regulation of Law No. 20 of 2014 Concerning Electronic Transactions
- Executive Bylaws of Law No. 9 of 2019 Regulating the Exchange of Credit Information

Oversight Authorities

- Communication and Information Technology Regulatory Authority (CITRA)
- Central Agency for Information Technology (CAIT)
- Central Bank of Kuwait (CBK)

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.

Kuwait recently repealed its Data Classification Policy, which is yet to be replaced. The Policy had established restrictions on cross-border transfers based on the classification of data into four tiers:

Public data (1), private insensitive data (2), private sensitive data (3), and highly sensitive data (4). Data tiers 3 and 4 were not allowed to be transferred internationally. Data tiers 1 and 2 could be transferred, albeit only with user consent.

Summary

- The Communications and Information Technology Regulatory Authority's Regulation on Data Privacy Protection, Cloud Computing Regulatory Framework, and Data Classification Policy (repealed) include provisions on cross-border data transfers. Since the Data Classification Policy was repealed, it was not replaced with an equivalent precise distinction of rules for the transfers of different types of data. The Data Protection Regulation, for instance, requires the disclosure of any transfer of personal data, including the specification of the countries to which data is transferred. It does not, however, specify transfer mechanisms. In addition, the National Cybersecurity Center requires organisations to categorise data into sensitive, restricted, and public classifications, to assess its sensitivity and significance, and to secure approval for processing sensitive data outside Kuwait.

Before the Data Classification Policy was repealed, data was classified in four tiers:

01. Tier 1: Public data, including information made publicly available online.
02. Tier 2: Private insensitive data, including name, age, and email address.
03. Tier 3: Private sensitive data, including legal documents and medical records.
04. Tier 4: Highly sensitive data, including encryption keys, political documents, and data relevant to national security.

- Data transfers outside Kuwait were prohibited for tiers 3 and 4 (see section on data localisation), while data of tiers 1 or 2 was allowed to be transferred with notification and consent from the data owner.
- Consent had to be given freely, upon information on the reason and destination of the transfer. Robust security measures had to protect the data during transfer.
- The Cloud Computing Regulatory Framework specified that subscribers of cloud services were responsible for classifying the data and ensuring that data tiers 3 and 4 were not hosted or stored outside Kuwait.
- The Subscribers Guide to Cloud Services outlined the process of choosing a service provider, the responsibilities and commitments of the subscriber. This framework stated that the responsibility for classifying data into four tiers and ensuring adherence to the corresponding security levels lies with the subscriber.

SOURCES

Secondary Legislation

- Communications and Information Technology Regulatory Authority: Data Privacy Protection Regulation
- Communications and Information Technology Regulatory Authority: Decision regarding the cancellation of the data classification policy
- Communications and Information Technology Regulatory Authority: The Data Classification Policy [repealed]
- Communications and Information Technology Regulatory Authority: The Cloud Computing Regulatory Framework
- Communications and Information Technology Regulatory Authority: The Cloud Service Providers Regulations and Commitments
- National Cybersecurity Center Resolution regarding the General National Framework Regulations for Electronic Data Classification (no source available)

Guidelines

- Communications and Information Technology Regulatory Authority: The Subscribers Guide to Cloud Services

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.

Kuwait recently repealed its Data Classification Policy, which is yet to be replaced. The Policy had established restrictions on cross-border transfers based on the classification of data into four tiers: Public data (1), private insensitive data (2), private sensitive data (3), and highly sensitive data (4). Data tiers 3 and 4 were not allowed to be transferred internationally. Data tiers 1 and 2 could be transferred, albeit only with user consent.

Summary

- The Communications and Information Technology Regulatory Authority's Regulation on Data Privacy Protection, Cloud Computing Regulatory Framework, and Data Classification Policy (repealed) include provisions on data localisation. Since the Data Classification Policy was repealed, it was not replaced with an equivalent precise distinction of rules for the localisation of different types of data.

  The Data Protection Regulation, for instance, requires the disclosure of any transfer of personal data, including the specification of the countries to which data is transferred. It does not, however, specify data localisation requirements. In addition, the National Cybersecurity Center requires organisations to categorise data into sensitive, restricted, and public classifications, to assess its sensitivity and significance, and to secure approval for processing sensitive data outside Kuwait.

  Before the Data Classification Policy was repealed, data was classified in four tiers:

  01 Tier 1: Public data, including information made publicly available online.

  02 Tier 2: Private insensitive data, including name, age, and email address.

  03 Tier 3: Private sensitive data, including legal documents and medical records.

  04 Tier 4: Highly sensitive data, including encryption keys, political documents, and data relevant to national security.

- Data transfers outside Kuwait were prohibited for tiers 3 and 4 (see section on data localisation), while data of tiers 1 or 2 was allowed to be transferred with notification and consent from the data owner. Consent had to be given freely, upon information on the reason and destination of the transfer. Robust security measures had to protect the data during transfer.

- The Cloud Computing Regulatory Framework specified that subscribers of cloud services were responsible for classifying the data and ensuring that data tiers 3 and 4 were not hosted or stored outside Kuwait.

SOURCES

Secondary Legislation

- Data Privacy Protection Regulation
- Communications and Information Technology Regulatory Authority: Decision regarding the cancellation of the data classification policy
- Communications and Information Technology Regulatory Authority: Data Classification Policy [repealed]
- Cloud Computing Regulatory Framework
- Cloud Service Providers Regulations and Commitments
- National Cybersecurity Center Resolution regarding the General National Framework Regulations for Electronic Data Classification (no source available)

Guidelines

- The Subscribers Guide to Cloud Services

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 regulated under the general consumer protection law. Implementing regulation confirms the law's application to online advertisement and sales. Rather than prohibiting specific practices, Kuwait grants consumer rights to safety, quality, information, and fair redress. There are no specific indirect obligations for e-commerce platforms. Spam is not generally prohibited, but allowed only during specific times and when accompanied by identifying information and an option to unsubscribe. Telecommunication and information technology service providers must create a database to stop such messages upon request. Oversight is divided between the Consumer Protection Department within the Ministry of Commerce and Industry and sectoral bodies.

Summary

- Kuwait has enacted various legislations to ensure comprehensive consumer protection. The Consumer Protection Law, in effect since 2014, provides robust protection for consumers, including rights to safety, quality, information, and redress. Additionally, the Constitution prohibits discrimination based on race, language, or religion, among others.

- The Executive Regulation of the Consumer Protection Law confirms the law's application to online advertisements and sales, ensuring that consumers are protected in digital transactions as well. It includes detailed articles and an annex that provide comprehensive guidance on the law's implementation, including specific procedures for compliance requirements, enforcement, and administrative processes.

- Complementing this, the Anti-Commercial Fraud Uniform System in the Gulf Cooperation Countries, effective since 2019, addresses acts such as producing, selling, or distributing counterfeit or substandard goods, and using fraudulent practices in trade.

- Kuwait implemented the Anti-Commercial Fraud Uniform System through the Law on the Anti-Commercial Fraud Uniform System in the Gulf Cooperation Countries of 2019. This law imposes strict penalties on violators, including fines and imprisonment, to deter fraudulent activities and protect consumers.

- The Executive Regulation of the Anti-Commercial Fraud Uniform System in the Gulf Cooperation Countries specifies procedures for businesses to comply with consumer protection standards, including documentation and reporting requirements.

- The Consumer Protection Department within the Ministry of Commerce and Industry oversees consumer protection by issuing licences, conducting inspections, and coordinating with relevant external authorities. Additionally, sector-specific regulation is overseen by the Communication and Information Technology Regulatory Authority for the telecommunications sector and the Central Bank of Kuwait for the financial sector.

- There are no specific guidelines on consumer protection by the Consumer Protection Department, although it regularly issues news items outlining consumer rights. The Central Bank of Kuwait and the Kuwait Banking Association launched an awareness campaign to highlight customer rights in interactions with banks.

SOURCES

Primary Legislation

- Law No. 39 of 2014 on Consumer Protection
- Law No. 20 of 2019 on the Anti-Commercial Fraud Uniform System in the Gulf Cooperation Countries
- The Constitution, Article 29 regarding Non-Discrimination

Secondary Legislation

- Ministry Of Commerce And Industry: Decision No. 27 of 2015 issuing the Executive Regulation of Law No. 39 of 2014 on Consumer Protection
- Ministry Of Commerce And Industry: Decision No. 106 of 2021 issuing the Executive Regulation of Law No. 20 of 2019 concerning the Anti-Commercial Fraud Uniform System in the Gulf Cooperation Countries
- Communication and Information Technology Regulatory Authority: The Regulation on the Protection of the Rights of Users of Telecommunication and Information Technology Services

Guidelines

- Central Bank of Kuwait: Let's be aware (awareness campaign)
- Ministry of Commerce and Industry: "Dear consumer" announcements

Oversight Authorities

- The Consumer Protection Department within the Ministry of Commerce and Industry
- The Communication and Information Technology Regulatory Authority
- Central Bank of Kuwait

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.

Kuwait has a dedicated law on electronic transactions that recognises electronic records, documents, messages, transactions, and signatures as equivalent to written ones. Exceptions apply to transactions regarding personal status and wills, as well as real estate. Kuwait differentiates between electronic signatures and protected electronic signatures, and establishes a mechanism for the approval of foreign authorities' certification of electronic signatures. Finally, Kuwait accepts electronic authentication and provides authentication through the Public Authority for Civil Information's "Kuwait Mobile ID" app.

Summary

- The Electronic Transactions Law, enacted in 2014, is the primary law that regulates electronic transactions in Kuwait. The law stipulates that electronic signatures, contracts, records, documents, messages and transactions have the same legal effect as their paper-based counterparts for civil, commercial, and administrative transactions. However, certain transactions are excluded, such as those related to personal status, real estate, promissory notes, and negotiable bills of exchange.

- The law distinguishes between standard electronic signatures and protected electronic signatures. Standard electronic signatures are legally binding if they meet essential criteria such as identifying the signatory, being linked to the signatory, and allowing detection of any alterations to the signed data.

- Protected electronic signatures must adhere to stricter requirements for security and integrity and, in turn, have the same effect as written signatures. They must be created using a secure signature tool, controlled exclusively by the signatory. Furthermore, changes in the data associated with the protected electronic signatures must be detectable.

- The role of e-authentication is primarily associated with protected electronic signatures. For these signatures, an electronic authentication certificate must be provided to validate the signature's authenticity. This certificate confirms the validity of the signature and the electronic document. The authentication process ensures that the electronic document's integrity and the signature's authenticity can be verified.
  The Public Authority for Civil Information (PACI) builds the infrastructure for electronic authentication and signatures. The Central Agency for Information Technology supervises providers of electronic authentication and signatures. The Central Bank of Kuwait (CBK) is responsible for the financial sector, issuing guidelines and resolutions related to electronic transactions.

- The Kuwait Mobile ID application, provided by PACI, serves as a key component of secondary legislation related to e-transactions. The application is a governmental authentication service that supports private transactions by providing secure digital identity verification.

- It facilitates various e-services by allowing users to authenticate their identity electronically, aligning with the requirements of the Electronic Transactions Law 2014. The Mobile ID application enhances the security and ease of electronic transactions by enabling reliable digital identification and authentication. Generally, providers have access to an online portal for registration and can register digitally.

SOURCES

Primary Legislation

- Law No. 20 of 2014 concerning Electronic Transactions

Secondary Legislation

- The Executive Regulation of Law No. 20 of 2014 concerning Electronic Transactions
- Public Authority for Civil Information: Kuwait Mobile ID

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.

Kuwait provides trade administration documents for imports in electronic form and enables electronic submission, through the Kuwait General Administration of Customs (KGAC) portal. The platform supports all documents in Arabic and also some documents in English. Kuwait is currently integrating various government agencies into a unified system, with the stated goal to achieve an Electronic Single Window. Finally, Kuwait applies simplified customs procedures for shipments valued below KWD 100, exempting such shipments from customs duties altogether.

Summary

- Kuwait's framework for paperless trade is supported by the Electronic Transactions Law, which grants electronic documents and signatures the same legal status as paper documents in customs procedures and facilitates the use of electronic records in commercial transactions, including those related to customs. The Executive Regulation of Electronic Transactions Law 2014 establishes the framework for implementing and enforcing the use of electronic records, signatures, and transactions.

- The Unified Customs Law of the Gulf Cooperation Council (GCC) States, issued in 2003, permits the electronic submission of customs declarations and associated documents. Kuwait enables importers to electronically submit trade documents such as invoices and certificates of origin via the Ministry of Commerce and Industry's portal and the Kuwait e-Government website.

- The Kuwait Customs Department supports this with an electronic platform for processing customs declarations and related activities. The Rules of Implementation of the GCC Common Customs Law aims to standardise customs processes, facilitate trade, and enhance economic integration within the GCC.

- Kuwait's electronic customs system integrates various government agencies for trade documentation but is not yet a fully implemented Single Window system.

- Low-value shipments in Kuwait, valued at KWD 100 or less, are exempt from customs duties, provided they are for personal use, not intended for commercial purposes, and are not received by businesses or professional traders.

- Kuwait Customs regularly publishes guidelines on the use of electronic systems for customs declarations, providing detailed instructions on electronic document submission, required technical standards, and digital authentication processes. These documents consist of a schedule detailing fees for customs inspection and IT services, a guide for declaring currency, and a comprehensive FAQ section.

SOURCES

Primary Legislation

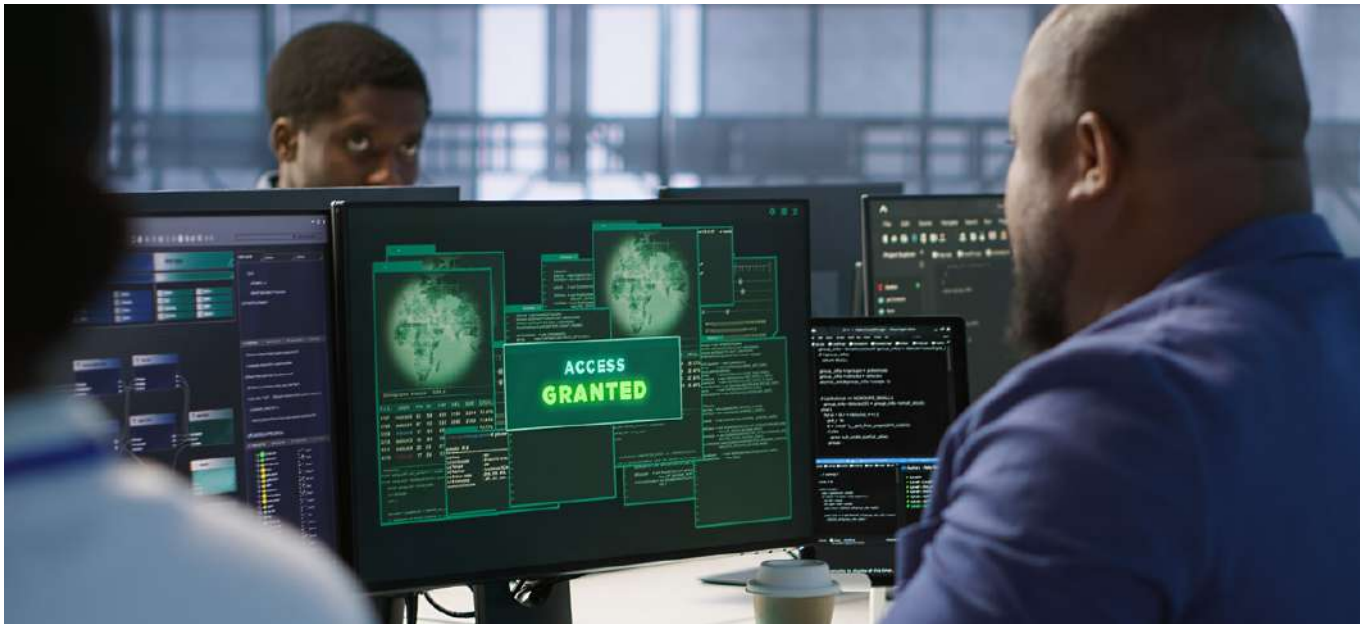
- The Law No. 20 of 2014 Concerning Electronic Transactions
- The Law No. 10 of 2003 on Issuing the Unified Customs Law of GCC States

Secondary Legislation

- The Executive Regulation of Law No. 20 of 2014 Concerning Electronic Transactions
- The Rules of Implementation of The Gulf Cooperation Council Common Customs Law
- Customs Instructions No. 94 of 2020 regarding the application of the minimum value of goods that do not meet the customs duty threshold

Guidelines

- Kuwait Customs: The Pricing Schedule for Handling Services for Customs Inspection Purposes and Computer System Services
- Kuwait Customs: The Currency Form Self-Declaration User Guide Document
- Kuwait Customs: Frequently Asked Questions



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.

Kuwait's law on combating information technology crimes focuses primarily on criminalising certain online conduct. For example, the law establishes penalties for the unauthorised access to and theft of data. The law does not demand incident notification. The data protection framework (see dedicated section), however, demands notification when personal data of a "large number" of users is improperly disclosed. Notification is required, towards authorities and users, as soon as possible or at the latest after 72 hours. Oversight is divided between the Electronic and Cyber Crime Combating Department under the Ministry of Interior and sectoral bodies.

Summary

- The Cybercrime Law criminalises actions such as unauthorised access to electronic systems, retrieval of personal data without permission, online fraud, distribution of pornography, and human trafficking via the internet. Additionally, it extends penalties from the Printing and Publishing Law to violations committed through information technology.

- This means that certain online activities are subject to the same penalties as traditional media violations, including mocking or defaming religion, criticising the Amir without authorisation, criticising the constitution, political figures, or representatives, and revealing state secrets.

- The Cyber Crime Combating Department under the Ministry of Interior oversees the implementation of Kuwait's Cybercrime Law. The Ministry of Interior works in coordination with other governmental bodies, such as the Communication and Information Technology Regulatory Authority (CITRA), a public authority with an independent corporate body and financial independence. CITRA plays a role in regulating the ICT sector and ensuring cybersecurity measures are in place.

- CITRA can draft rules, enforce compliance, and impose penalties. According to the Cybercrime Law, the public prosecution is responsible for investigating and prosecuting cybercrime offences, ensuring that cybercriminals are held accountable. Other authorities, including the Central Bank of Kuwait, oversee cybersecurity within their sectors.

- The Central Bank of Kuwait introduced the Cyber Security Framework for the banking sector, which provides detailed guidelines, recommendations, and procedures to ensure effective internal controls and robust cybersecurity measures within banks.

- The National Cybersecurity Strategy 2017-2020, issued by CITRA, outlined Kuwait's cybersecurity approach, detailing goals, priorities, and responsibilities. The strategy emphasises collaboration between the government and private sector to enhance cyber resilience. The National Cybersecurity Center oversees Kuwait's cybersecurity strategy, protecting government networks and critical infrastructure.

- The Electronic and Cyber Crime Combating Department under the Ministry of Interior provides awareness brochures on various topics, including punishments for cyber crime, payment card fraud, reporting and verification of information, privacy, downloading programs and opening files, and computers in shared networks. These brochures aim to educate the public on cybersecurity and encourage proactive measures to safeguard against cyber threats.

SOURCES

Primary Legislation

- Law No. 63 of 2015 on Combating Information Technology Crimes
- Law No. 3 of 2006 on Press and Publications

Secondary Legislation

- Central Bank of Kuwait: The Cyber Security Framework for Kuwaiti Banking Sector

Guidelines

- Communication and Information Technology Regulatory Authority: The National Cybersecurity Strategy
- Ministry of Interior: Awareness Brochures by the Electronic and Cyber Crime Combating Department

Oversight Authorities

- The Communication and Information Technology Regulatory Authority
- The Electronic and Cyber Crime Combating Department under the Ministry of Interior
- The Public Prosecution
- The Central Bank of Kuwait
- National Cybersecurity Center

Artificial Intelligence

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

Guiding Questions

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

There is currently no binding framework devoted to the governance of AI. Kuwait is in the process of developing its framework for AI regulation. Regulatory agencies have not yet released specific guidance on how existing rules for the digital economy apply to AI. Recently, the Supreme Council for Planning and Development released the Government AI Readiness Index, while the Central Bank of Kuwait issued a report on advantages and challenges of AI.

Summary

- There is currently no binding framework devoted to the governance of AI. Kuwait is developing its legal framework for AI, with ongoing efforts to establish comprehensive regulations. There is currently no dedicated regulator.

  In the interim, several existing regulatory bodies intersect with AI. The Communications and Information Technology Regulatory Authority manages the telecommunications sector and develops IT policies.

- It issued a Guide to AI Ethics that establishes ethical principles for AI use, focusing on respect for individuals, adherence to Islamic law, the constitution, environmental sustainability, and the peaceful application of AI.

- It emphasises transparency, accountability, data protection, inclusivity, and non-discrimination in AI development and implementation. The Central Agency for Information Technology executes these rules. The Central Bank of Kuwait oversees the financial sector.

- The National Development Research Center (NDRC) under the General Secretariat of the Supreme Council for Planning and Development has released a report about the Government AI Readiness Index 2023, highlighting Kuwait's ongoing efforts to enhance digital governance and AI capabilities.

- Additionally, the Central Bank has issued a report on advantages and challenges of AI. This report covers several key areas, including the impact of AI technology on GDP and global investments, its

- effects on employment across different economies, and the potential applications of AI for central banks to enhance operations and ensure financial stability. It also discusses various AI applications that improve the quality of banking and financial services, with examples from global banks, and addresses the economic and social challenges posed by AI technology.

SOURCES

Guidelines

- The General Secretariat of the Supreme Council for Planning and Development: A report about the Government AI Readiness Index 2023
- Central Bank of Kuwait: Artificial Intelligence "Advantages and Challenges"
- Communications and Information Technology Regulatory Authority: Guide to Artificial Intelligence Ethics

Oversight Authorities

- The Communication and Information Technology Regulatory Authority
- The Central Agency for Information Technology
- The Central Bank of Kuwait

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.

Kuwait's copyright law provides protection for "computer programs", foreseeing exceptions for personal use and educational purposes. Kuwait does not generally mandate the sharing of source code. Access to source code for critical applications in the banking sector is permissible if managed by storing the code on premises, through an escrow arrangement, or with strict contractual terms with the application/service provider. The government can request access to digital information, including software, in cybercrime investigations. In addition, the government may require source code provision for participation in public tenders concerning sectors critical to national security or public safety.

Summary

- The Law on Copyright and Related Rights 2019 explicitly includes source code within its protection of computer programs. This law recognises source code as a form of literary work, providing it with copyright protection. The Law on Copyright and Related Rights 2019 allows for certain exceptions to copyright protection.

- These exceptions include personal use, educational purposes, and private study, provided that such uses do not affect the normal exploitation of the work or unfairly harm the author's rights. Additionally, the law allows for some limited use of copyrighted works for educational purposes under specific conditions.

- The Law on Electronic Transactions 2014 supports the protection of digital works, including software, ensuring that electronic records and data hold the same legal status as traditional documents.

- Kuwait does not establish general statutory requirements for mandatory source code sharing. The legal framework does not impose a broad obligation on companies or individuals to disclose source code.

- However, contractual obligations may arise, especially in government contracts, where developers might be required to provide source code. These requirements are usually specified within contracts rather than dictated by statute. Private agreements thus cover the handing over of software after the conclusion of a contract.

- In addition to these laws, Kuwait's Cyber Security Framework for the banking sector outlines specific measures for managing access to critical application source code. These include storing the code on-premises, utilising an escrow arrangement, or setting strict contractual terms with the service provider.

- The framework also emphasises the importance of thorough testing, covering user management, application and infrastructure security, source code reviews, penetration testing, and vulnerability assessments.

- Moreover, the Law on Combating Information Technology Crimes grants the government authority to request access to digital information, including software, under specific circumstances, particularly in matters related to national security or investigations into cybercrime.

SOURCES

- Law No. 75 of 2019 on Copyright and Related Rights, Kuwait [other government source]
- The Law No. 20 of 2014 Concerning Electronic Transactions
- Law No. 63 of 2015 on Combating Information Technology Crimes
- Law No. 49 of 2016 regarding public tenders and its amendments issued by Law No. 74 of 2019 and its executive regulations for the State of Kuwait
- Central Bank of Kuwait: The Cyber Security Framework for Kuwaiti Banking Sector

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.

Kuwait does not impose import-related fees or indirect taxes on digital services or digital products. Regarding e-commerce imports, Kuwait imposes a standard customs duty, above a de minimis threshold of KWD 100, but no indirect taxes. Kuwait is currently laying the foundation for a future value-added tax. It does not impose direct taxes specifically on providers of digital services or digital products, instead levying corporate tax. Electronic registration is not generally possible for foreign providers.

Summary

- Kuwait imposes customs duties on physical goods, rather than digital services (e.g., software downloads, streaming services). The standard customs duty of 5% applies to most imported goods, including e-commerce imports. Certain items, such as basic foodstuffs and medicines, among others, are exempt from customs duties. Additionally, handling and processing fees may apply for the clearance of imported goods. Imports valued below KWD 100 are exempt from customs duties.

- Kuwait is also an active participant in the Gulf Cooperation Council (GCC) and the GCC Customs Union. The Unified Customs Law of the GCC States aligns Kuwait's customs procedures with those of other GCC member states, providing a consistent framework for customs regulations and tariffs.

- The Rules of Implementation of the GCC Common Customs Law establish a unified legal framework for customs procedures across the GCC member states, including Kuwait. These rules aim to standardise customs processes, facilitate trade, and enhance economic integration within the GCC.

- Finally, Kuwait has established specific bilateral agreements with various Arab and other nations to streamline customs procedures. These agreements generally encompass provisions for the mutual recognition of customs documentation, the reduction of tariffs on certain goods, and enhanced cooperation in customs enforcement.

- Kuwait has not currently implemented a value-added-tax (VAT). Kuwait is a signatory to the GCC VAT Framework Agreement, which lays the groundwork for future VAT implementation. This agreement establishes the primary regulations for implementing VAT in the GCC, permitting a standard VAT rate of 5%, while certain goods and services may be zero-rated or exempt from VAT.

- Kuwait does not currently impose direct taxes specifically on providers of digital services or digital products, instead relying on corporate income tax. The Income Tax Decree as well as the Ministry of Finance's tax guidelines establish the specifics of this direct taxation.

  Finally, Kuwait is a signatory to the Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting and has entered into several double taxation avoidance agreements.

SOURCES

Primary Legislation

- The Law No. 2 of 2008 on Amending some Provisions of Kuwait Income Tax Decree No. 3 of 1955
- The Kuwait Income Tax Law in the concerned region No. 23 of 1961
- The Law No. 10 of 2003 on Issuing the Unified Customs Law of GCC States

Secondary Legislation

- The Executive Bylaw of Law No. 2 of 2008 Amending some provisions of the Income Tax Decree No. 3 of 1955
- The Executive Rules and Instructions of Kuwaiti Income Tax Decree No. 3 of 1955 and amended by Law No. 2 of 2008
- The Executive Rules and Instructions of the Income Tax Decree No. 3 of 1955 and its amendments (Executive Rule No. 53) regarding the method of payment of taxes and fines
- The Rules of Implementation of The GCC Common Customs Law

Guidelines

- Ministry of Finance: Corporate Services Implementation Procedures Guide
- Ministry of Finance: Institutional Services Implementation Procedures Guide
- General Administration of Customs: The Pricing Schedule for Handling Services for Customs Inspection Purposes and Computer System Services
- General Administration of Customs: The Currency Form Self-Declaration User Guide Document
- General Administration of Customs: Frequently Asked Questions
- General Administration of Customs: The Unified Guide for Advance Ruling
- General Administration of Customs: The Unified Guide for Customs Procedures at First Points of Entry into the Member States of the Cooperation Council for the Arab States of the Gulf (GCC)
- General Administration of Customs: The Pricelist Guide
- General Administration of Customs: List of exempted goods in the State of Kuwait
- General Administration of Customs: List of prohibited goods in the State of Kuwait (Foodstuffs, animals, marine, plants, medicines and the like)
- General Administration of Customs: List of prohibited goods in the State of Kuwait (Other goods)
- General Administration of Customs: Customs Tariff Search (HS code)

International Frameworks

- The Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (MLI)
- The Common VAT Agreement of the States of the Gulf Cooperation Council (GCC)
- Ministry of Finance: International Agreements
- The Common Customs Law of the GCC States
- A list of customs instructions issued regarding bilateral agreements between the State of Kuwait and some Arab countries
- A list of customs instructions issued regarding bilateral agreements between the State of Kuwait and some Foreign countries
- The GCC Customs Union

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.

There is no specific regulatory framework for digital payments. Rather, the electronic transactions framework applies, along with the law on anti-money-laundering and counter-terrorism-financing, as well as regulations by the central bank. The central bank issued the Instructions for Regulating the Electronic Payment of Funds, which include anti-money-laundering and counter-terrorism-financing requirements. These requirements apply to payment service providers, limited purpose e-money providers, and local banks. In addition, entities that offer electronic payment services must register with the central bank.

Summary

- The Electronic Transactions Law, enacted in 2014, is the primary legislation addressing digital payments in Kuwait. This law governs electronic transactions, digital contracts, and e-commerce, covering both the public and private sectors.

- It mandates that any regulated entity engaged in electronic payments must comply with requirements set by the Central Bank of Kuwait, as well as the Anti-Money Laundering and Counter-Terrorism Financing Law. Additionally, these institutions must take the necessary procedures to provide safe services to customers while maintaining banking secrecy in accordance with legal standards.

- In 2023, the Central Bank of Kuwait (CBK) promulgated the Instructions for Regulating the Electronic Payment of Funds, updating the previous regulations issued in 2018.

- These instructions, under the umbrella of the Electronic Transactions Law 2014, entrust the CBK with full oversight and supervision of electronic payment transactions, as well as the authority to issue binding instructions. The instructions apply to all payment service providers, limited purpose e-money providers, and local banks.

  They also include supervisory controls that regulated entities must adhere to when practising e-payment or e-money activities, or operating e-payment systems. These controls cover areas

  such as corporate governance, risk management, anti-money laundering (AML) and countering the financing of terrorism (CFT), cybersecurity, business continuity, and customer protection. Institutions must comply with AML/CFT obligations as outlined in the CBK Instructions Regulating the Electronic Payment of Funds.

- Service providers must align with the requirements under the Law on Anti-Money Laundering and Combating the Financing of Terrorism, ministerial resolutions, international standards like those of the Financial Action Task Force (FATF), and any further instructions from the CBK or related supervisory bodies.

- Secondary legislation for digital payments encompasses various resolutions and circulars issued by the Central Bank of Kuwait, such as the resolutions from 2018 and 2023 which regulate electronic payments.

- Several circulars address specific areas such as fraud reporting, prohibition of customer fees, and requirements for digital payment services conducted outside Kuwait. They also cover guidelines for Buy Now Pay Later services, cyber security, and the provision of Point of Sales devices. These regulations collectively ensure secure, compliant, and efficient digital payment systems.

- The Central Bank of Kuwait offers an e-payment services portal, enabling regulated entities to access regulatory information and guidelines. Additionally, the CBK has issued guidelines for digital banks, which are anticipated to enhance the adoption of digital payments by providing advanced and secure payment solutions.

- Kuwait engages in international frameworks for digital payments, aligning its systems with global standards like ISO/IEC for security and interoperability. It participates in the SWIFT network for cross-border payments, is a member of the IBAN system for standardised bank account numbers, and collaborates with the International Monetary Fund and World Bank to promote financial stability and innovation.

- Kuwait follows United Nations and International Telecommunication Union guidelines for secure financial services and supports World Trade Organization practices for trade-compatible payment systems.

- Regionally, Kuwait partners with the Arab Monetary Fund, and Gulf Cooperation Council (GCC) initiatives like the AFAQ Gulf payments system, GCCNET, and Buna Payment Platform, enhancing cross-border transactions across the region.

SOURCES

Primary Legislation

- The Law No. 20 of 2014 Concerning Electronic Transactions
- The Law No. 32 of 1968 Concerning Currency, The Central Bank of Kuwait And The Regulation Of Banking
- The Law No. 106 of 2013 on Anti-Money Laundering and Combating the Financing of Terrorism
- The Law No. 63 of 2015 on Combating Information Technology Crimes

Secondary Legislation

- The Resolution No. 45/471 of 2023 Promulgating the Instructions Regulating the Electronic Payment of Funds
- The Resolution No. 44/430 of Year 2018 Promulgating Instructions for Regulation the Electronic Payment of Funds
- The Circular No. (2/BS/IBS/475/2021) to all Local Banks and Electronic Payment Infrastructure Providers (EPIPs) Regarding the Report of Frauds on Payment Cards
- The Circular to all E-Payment Infrastructure Providers (EPIPs) and their Agents Concerning Prohibition Against Collecting Fees and Charges from the Customer (The End User)
- The Circular No. (2/BS, IBS, ES/520/2023) to all Local Banks and Electronic Payment Infrastructure Providers and their agents concerning the Electronic Payment Links for Individual Clients
- The Circular No. (2/BS, IBS, FS, FS, ES/525/2023) to all local Banks, Financing Companies and Large Electronic Money Service Providers Concerning Regulations for Buy Now Pay Later Services (BNPL)
- The Circular No. (2/SE/526/2023) to all E-Payment Service Providers, E-Money Service Providers, and E-Payment Service Operators Concerning Controls for Appointing Leadership Position
- The Circular No. (2/SE/527/2023) to All E-Payment Service Providers and E-Money Service Providers Concerning Instructions on Minimum Cyber Security and Business Continuity Requirements
- The Circular No. (2/SE/529/2023) to All E-Payment Service Providers and E-Money Service Providers Concerning AML/CFT Instructions
- The Circular No. (2/BS, IBS, ES/531/2023) to all Local Banks, E-Payment Service Operators, E-Payment Service Providers and E-Money Service Providers regarding MCC Codes and Description of Payment Transactions
- The Circular No. (2/ES/532/2023) to E-Payment Service Operators, E-Payment Service Providers, and E-Money Service Providers Regulating the Provision of POS and Soft POS Devices to Exhibition Organizers
- The Circular to all E-Payment Service Providers, E-Money Service Providers and E-Payment Service Operators Concerning Accessing the KwFIU Website to Update the Suspicion Indicators that Helps in Monitoring Suspicious Transactions
- - The Circular No. (2/ BS, IBS/535/2023) to all local Banks on Linking with the Shared Electronic Banking Services Company (KNET) for the Apple Pay Service

Guidelines

- The e-Payment Services Portal
- Guide to establishing digital banks in the State of Kuwait

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.

Kuwait has implemented measures specifically targeting SME participation in digital trade. While the government has established a general framework for SME development, evidence of direct digital economy support initiatives remains sparse. The primary mechanism for SME assistance is a national fund, which has begun to incorporate digital elements into its offerings.

Summary

- The Kuwait National Fund for SME Development, established in 2013 with a capital of USD 7 billion, serves as a cornerstone of Kuwait's SME support structure. This fund provides a range of financial and operational support services to SMEs across various sectors. While not exclusively focused on digital trade, the fund has begun to incorporate digital elements into its portfolio of services.

- One digital initiative under the National Fund's purview is a partnership with Agility, a global logistics provider. This collaboration has resulted in the creation of an online portal designed to facilitate SMEs' entry into e-commerce.

  The portal offers small businesses expedited access to resources necessary for establishing and expanding electronic storefronts, thereby supporting their digital sales capabilities.

- The Kuwait Vision 2035, announced in 2017, sets forth the broader economic framework within which SME development is situated. This strategic plan aims to establish Kuwait as an international financial and trading hub. Whilst the vision does not explicitly detail digital support interventions for SMEs, such measures may be developed as part of the ongoing implementation of this long-term strategy.

- The government documents the targets and progress of Vision 2035 on the New Kuwait website, providing a platform for potential future digital inclusion initiatives.

  It is important to note that beyond these initiatives, there is limited publicly available information on specific programmes or services directly supporting SMEs or disadvantaged groups in leveraging digital trade opportunities in Kuwait. The current landscape suggests a nascent approach to digital trade support for SMEs, with potential for further development in line with Kuwait's broader economic objectives.

SOURCES

- New Kuwait
- The National Fund for Small and Medium Enterprise Development
- Agility: Kuwait National Fund Help Small Businesses Sell Online
- SAP: Developing Kuwaiti Technology Skills

02
Digital Economy Factsheet

Digital Economy Factsheet

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

Advanced technology products accounted for 14.72% of Kuwait's imports. The share of advanced technology products in exports was considerably lower at 0.8%, indicating a technology trade imbalance.

Figure 1: Telecommunications, Computer, Information and Audiovisual Services

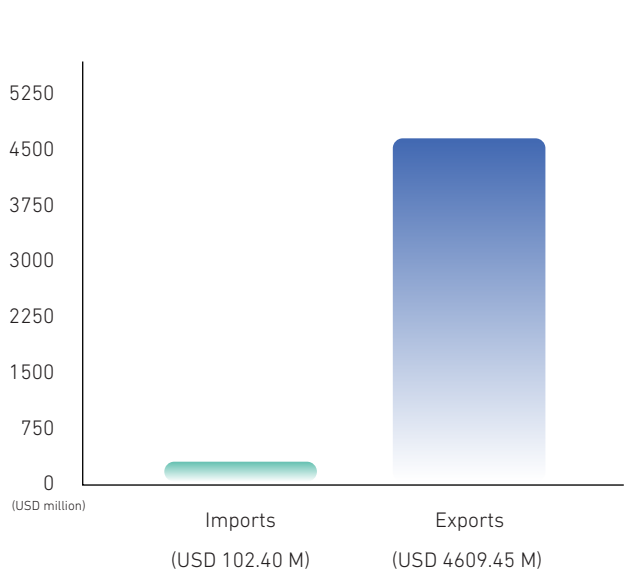


Figure 1 provides data for Kuwait's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

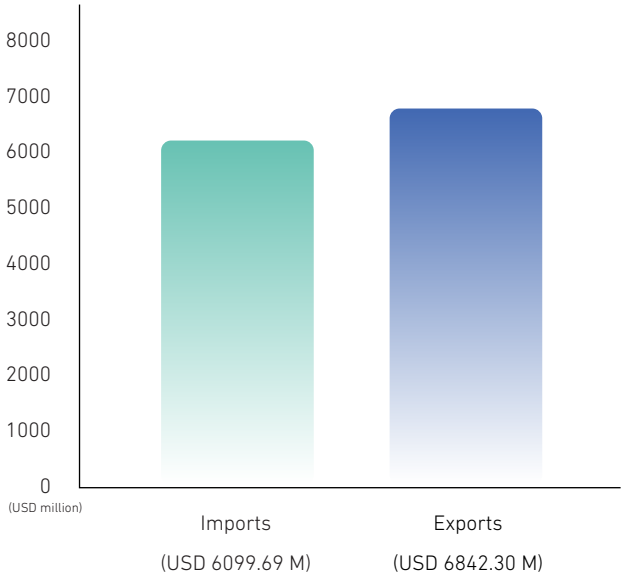


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Kuwait'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

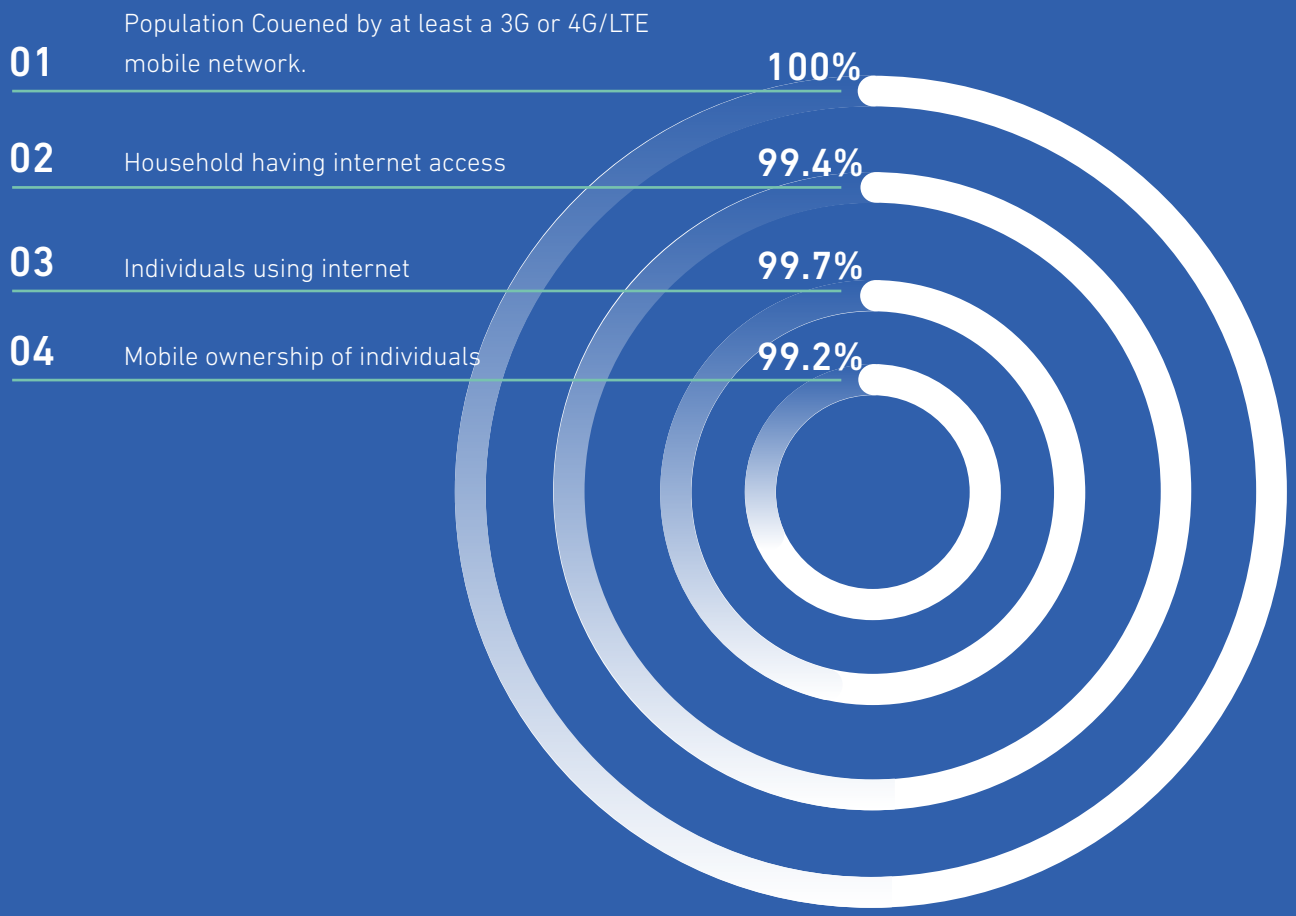


Figure 3 provides data to analyze Kuwait's digital infrastructure and connectivity in 2022.

Digital Skills

To document Kuwait'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 61.56% in 2021, indicating high participation in higher education. The adult literacy rate was 96% in 2020. Government expenditure on education as a percentage of GDP was 3.16% in 2022.

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

- 71.71% were able to copy or move a file or folder (2019).
- 31.13% had created electronic presentations with presentation software (2021).
- 65.09% could find, download, install and configure software (2021).

Digital Government

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

In terms of digital government services in 2022, Kuwait had only a cloud strategy/policy with no platform yet. It did not have a government interoperability framework. It did not have a government open-source software policy or action plan. Kuwait did not maintain an open government portal but did have an open data portal.

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

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

01 It had a government technology or digital transformation strategy in draft or planned

02 It had both a strategy and program to improve digital skills in the public sector

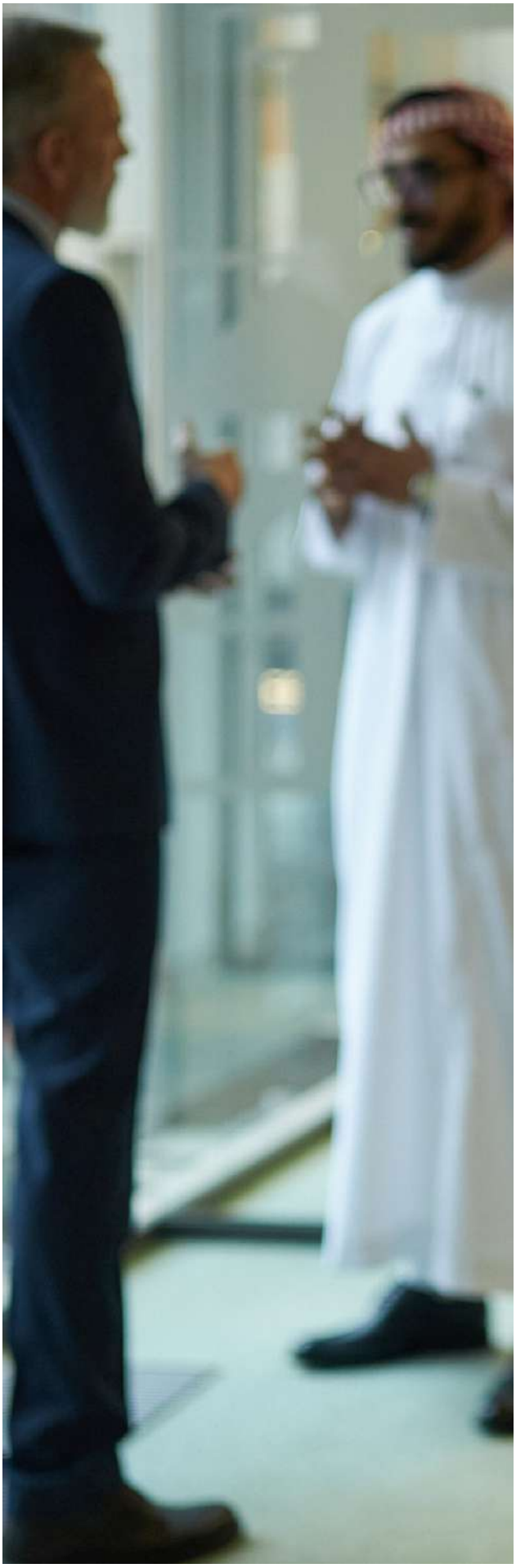
03 It did not have strategies or programs to improve public sector innovation

03 International Commitments and Collaboration

International Commitments and Collaboration

The purpose of this section is to outline the existing international commitments of Kuwait 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

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

Conventions

Kuwait is party to the following conventions and agreements:

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

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

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

04 Gulf Cooperation Council Unified VAT Agreement (Taxation)

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

06 Gulf Cooperation Council Common Customs Law (Customs Duties)

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

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

Guidelines, Recommendations, and Principles

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

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

02 United Nations Educational, Scientific and Cultural Organization Recommendation on the Ethics of Artificial Intelligence (Artificial Intelligence)

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

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

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

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

07 ESCWA Guideline on personal data protection (Data protection)

08 ESCWA Guideline on cybercrime (Cybersecurity)

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

Models

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

Other Commitments

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

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

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

05 ISO 22376:2023 (Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal data format for authentication, verification and acquisition of data carried by a document or object) (Cybersecurity)

06 ISO 31700-1:2023 (Consumer protection — Privacy by design for consumer goods and services) (Consumer protection)

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

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

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

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

Fora

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

01 United Nations Global Digital Compact (Cross-cutting)

02 Arab Federation for Digital Economy (Cross-cutting)

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

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

05 Buna Payment System (Electronic payments)

@dcorg | www.dco.org