Saudi Arabia

Digital Trade Acceleration Initiative

Country Report

Disclaimer

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

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

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

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

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

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

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

How to Read This Report

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

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

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

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

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

Table of Contents

01 Domestic Regulatory Environment Assessment 6

Data Protection 7
Cross-Border Data Transfers 12
Location of Computing Facilities 15
Online Consumer Protection 18
Electronic Transactions 21
Trade Facilitation with Digital Means 24
Cybersecurity 27
Artificial Intelligence 31
Source Code 34
Digital Economy Taxation and Customs Duties 37
Electronic Payments 40
SMEs and Digital Inclusion 43

02 Digital Economy Factsheet 46

Size and Activities of the Digital Economy 47
Digital Infrastructure and Connectivity 48
Digital Skills 49
Digital Government 50

03 International Commitments and Collaboration 52

Commitments 53
Fora 55

EXECUTIVE SUMMARY

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

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

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

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

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

Data Protection:

Consent is required for data processing but alternatives are provided, including the legitimate interest of the data controller. Data subjects are entitled to rights including information access, rectification, and deletion. Data processors are required to appoint a data protection officer, in specific cases, and the government maintains a national register of data controllers.

Cross-Border Data Transfers:

Cross-border data transfers are allowed through several mechanisms, as long as they do not prejudice national security. Transfers are allowed to countries with an adequate data protection level. To other countries, transfers are enabled by safeguards, such as standard contractual clauses, certification, and binding codes of conduct. In exceptional cases, transfers are allowed without either adequacy or safeguards, for example to protect vital interest.

Location of Computing Facilities:

Saudi Arabia does not generally require data to be localised. Specific data localisation regimes apply regarding government data, as well as data regarding insurance, accounting, and employer records.

Online Consumer Protection:

Online consumers are protected under the E-Commerce Law, which prohibits practices such as misleading consumers. E-commerce platforms must uphold transparency requirements regarding their terms and conditions. The sending of unsolicited messages (spam) is generally prohibited and promotional messages must include contact details and an unsubscribe option.

Electronic Transactions:

Saudi Arabia establishes the validity and enforceability of electronic transactions, records, and signatures. Exceptions apply, for example transactions regarding personal status. The framework does not differentiate between different types of electronic signatures.

Trade Facilitation with Digital Means:

Saudi Arabia provides trade administration documents in electronic form and enables electronic submission. The National Single Window is operational.

Cybersecurity:

Saudi Arabia establishes cybersecurity obligations, including incident notification requirements towards authorities. Several offences in cyberspace are criminalised, with a tiered penalty system based on the gravity of offences.

Artificial Intelligence:

There is currently no specific binding framework on the governance of AI. The government has focused on enhancing the local AI sector as well as government use of AI in several non-binding policy documents, for example the National Strategy for Data and AI.

Source Code:

The copyright law protects computer programs, granting authors exclusive rights, subject to exceptions. Saudi Arabia does not mandate any form of source code sharing.

Digital Economy Taxation and Customs Duties:

Digital services or digital products are not subject to customs duties but are subject to value-added tax. E-commerce imports are subject to both customs duties and value-added tax. There are no specific direct taxes on providers of digital services/products.

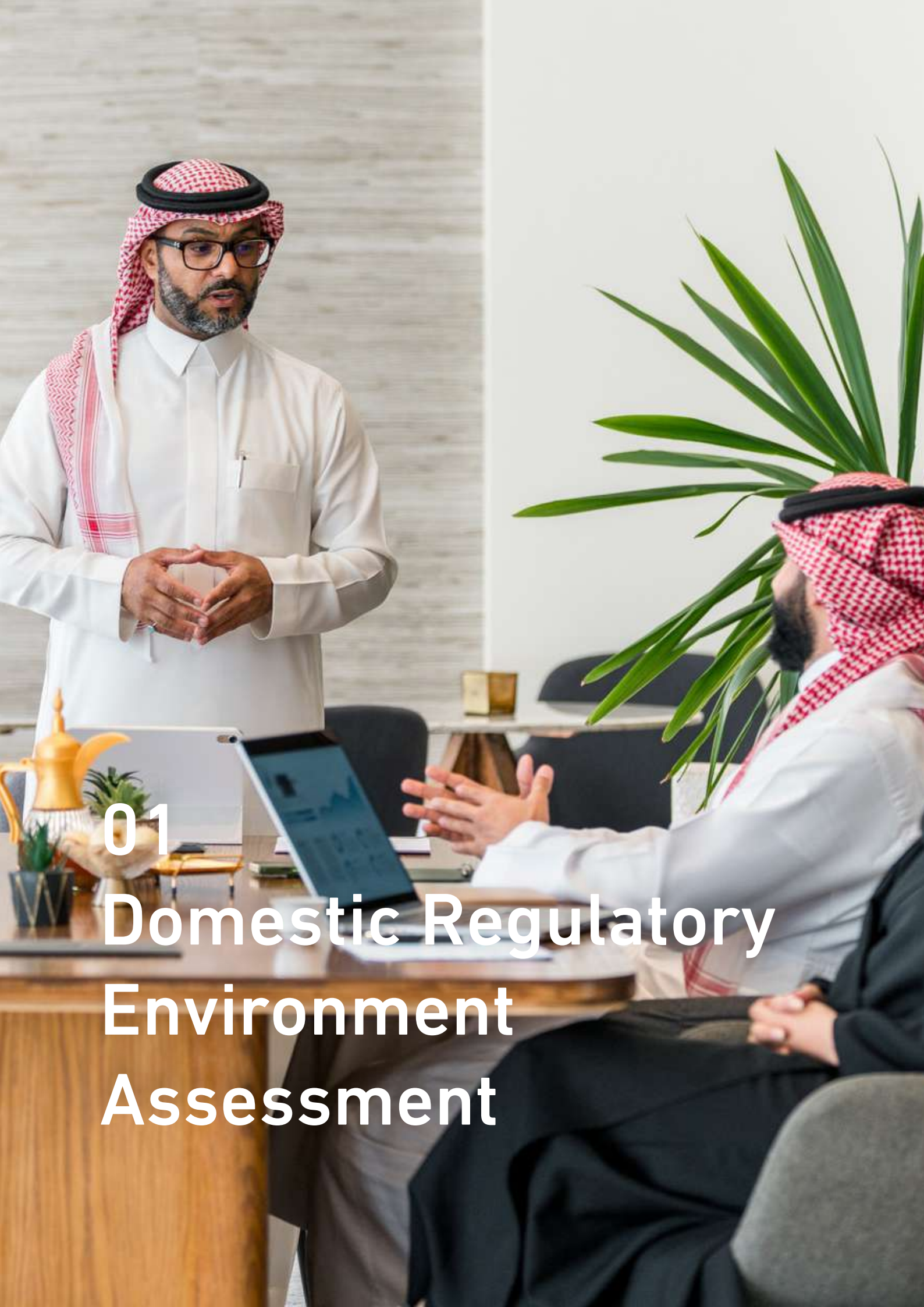
Electronic Payments:

Know-your-customer, anti-money-laundering, and counter-terroism-financing rules apply to electronic payment providers. A licence, issued by the central bank, is required to provide electronic payment services.

SMEs and Digital Inclusion:

Saudi Arabia has implemented a range of initiatives to support SMEs and disadvantaged groups in digital trade as part of its Vision 2030 strategy.

The Saudi government emplovarious policy instruments, including financial support through loans and grants, regulatory measures like fee caps to encourage electronic payments, capacity building through training and technical support, infrastructure development via innovation centres and entrepreneurship hubs, and targeted programmes for women entrepreneurs and specific sectors such as manufacturing.



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.

Saudi Arabia's data protection law requires consent for data processing but provides exceptions, including processing for the legitimate interest of the controller and for compliance with legal obligations or an agreement with the data subject. Data subject rights are granted the rights to information, access, rectification and deletion. Data processors are required to appoint a data protection officer, in cases specified by regulation, and the government maintains a national register of data controllers. The Saudi Data and AI Authority as well as sectoral bodies are in charge of oversight.

Summary

- The Personal Data Protection Law will enter into force in September 2024, following an amendment and postponement. The law covers entities collecting or processing the data of individuals located in Saudi Arabia, including deceased people.

- Such entities must register, conduct a privacy impact assessment, and obtain data subjects' consent (with exceptions). Data subjects are granted the rights to information, rectification, access, deletion, and consent withdrawal.

- The Saudi Data and AI Authority (SDAIA) is an independent agency responsible for implementing the Personal Data Protection Law. The SDAIA issued the Implementing Regulation of the Personal Data Protection Law. The regulation specifies data subject rights, processes related to data breaches, and provisions on health and credit data, among others.

The SDAIA adopted various rules and guidelines to specify data protection requirements:

01 The Rules for Appointing Personal Data Protection Officers state that the controller must provide the competent authority with the DPO's contact details immediately upon their appointment, through the National Data Governance Platform.

02 The Personal Data Destruction, Anonymisation, and Pseudonymisation Guideline assists controllers in complying with the specific requirements.

03 The Personal Data Protection Law Guide aids controllers with general compliance.

04 Other guidelines, including some that are currently under deliberation, cover personal data processing activities records, registration procedures, and minimum personal data determination (see full list in sources below).

05 Beyond the data protection law, the SDAIA issued other data protection frameworks, most of which precede the law:

06 The Data Management and Personal Data Protection Standards applies to government data and covers 15 domains such as data governance, quality, operations, and document and content management.

05 The National Strategy for Data and AI aims to place Saudi Arabia as an industry leader and a leading economy utilising and exporting data and AI.

06 The National Data Governance platform assists organisations in determining whether it is mandatory for them to appoint a data protection officer and conduct privacy impact assessment, among other obligations.

07 The Freedom of Information Policy and Regulations include guiding principles of data freedom and apply to requests made by individuals to access or obtain unprotected public data generated by public entities.

The Privacy Policy Guideline guides entities through the preparation and development of their privacy policy, ensuring compliance with the right to information.

- The Data Classification Policy categorises government data in 4 levels: top secret, secret, restricted, and public.

  The Data and Privacy Regulatory Sandbox aims to support entities who are creating products and solutions that utilise personal data in innovative and safe ways.

- The Data Sovereignty Public Policy, which is currently under consultation, aims at setting the fundamental principles that ensure the preservation of Saudi Arabia's sovereignty over its data while developing, enabling, and harnessing data.

- The Guidelines on the Secondary Use of Data, on which a consultation was held in 2023, regulates data sharing for research, development, and innovation.

Other relevant authorities, with which the SDAIA collaborates, include:

01 The Saudi Central Bank, which oversees data protection within the financial sector. The Saudi Central Bank established the Implementing Regulations for the Credit Information Law, as well as the regulations of work procedures and litigation before the Committee for Consideration and Settlement of Credit Information Violations and Disputes.

02 The Communications and Information Technology Commision, which regulates data protection issues related to telecommunications and ICT.

03 The Public Prosecution, which investigates and prosecutes cases in the competent court, which in turn issues penalties.

04 The Communication, Space and Technology Commission, which issued the Amended User Protection Regulations, striving for services of appropriate quality, providing protection from harmful content, and maintaining the confidentiality of communications.

SOURCES

Primary Legislation

- Saudi Data and AI Authority: Personal Data Protection Law of 2021 (amended in 2023)
- Saudi Central Bank: Credit Information Law of 2008
- Communications and Information Technology Commission: Law of Telecommunications and Information Technology 2022

Secondary Legislation

- Saudi Data and AI Authority: The implementing regulation of the Personal Data protection Law
- Saudi Data and AI Authority: Regulation on Personal Data Transfer outside the Kingdom
- Saudi Data and AI Authority: Rules for Appointing Data Protection Officer
- Saudi Data and AI Authority: Freedom of Information Policy and Regulations
- Communication, Space and Technology Commission: The Amended User Protection Regulations
- The Regulatory Arrangements of the Saudi Data & AI Authority

Guidelines

- Saudi Data and AI Authority: Data Management and Personal Data Protection Standards
- Saudi Data and AI Authority: National Strategy for Data and AI
- Saudi Data and AI Authority: National Data Governance Platform
- Saudi Data and AI Authority: Personal Data Protection Law Guide
- Saudi Data and AI Authority: Rules Governing the National Register of Controllers
- Saudi Data and AI Authority: Personal Data Destruction, Anonymization, and Pseudonymisation Guideline
- Saudi Data and AI Authority: Personal Data Processing Activities Records Guideline
- Saudi Data and AI Authority: Minimum Personal Data Determination Guideline
- Saudi Data and AI Authority: The Data and Privacy Regulatory Sandbox.
- Saudi Data and AI Authority: The Data Sovereignty Public Policy
- Saudi Data and AI Authority: Secondary Use of Data Guidelines
- Saudi Data and AI Authority: Data Classification Policy
- Saudi Data and AI Authority: Elaboration and Developing Privacy Policy Guideline

Oversight Authorities

- Saudi Data and AI Authority
- Saudi Central Bank
- Communications, Space and Technology Commission

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.

In Saudi Arabia, cross-border data transfers are subject to specific rules and allowed through several mechanisms, as long as they do not prejudice national security. Transfers are allowed to countries whose data protection level is designated as at least equal to Saudi Arabia's by the government. To other countries, transfers are enabled by safeguards, such as standard contractual clauses, certification, and binding codes of conduct. Finally, in exceptional cases, transfers are allowed without either adequacy or safeguards, for example transfers that protect the data subject's vital interest or are necessary to fulfil a contract with the data subject. No special conditions apply to transfers of specific data types.

Summary

- The Personal Data Protection Law establishes conditions for cross-border data transfers, which are specified in the recently amended Regulation on Personal Data Transfer outside the Kingdom.

  Several mechanisms enable data transfers, provided that they do not impact national security or vital interests of Saudi Arabia, and do not violate other laws – shifting away from the single transfer approval mechanism.

- Transfers to countries whose data protection level is designated as at least equal to Saudi Arabia's are generally allowed. The Saudi Data and AI Authority (SDAIA) is to publish a list of countries or international organisations that provide such appropriate protection and to review this list every four years.

- Transfers to countries without adequate data protection levels are allowed if the controller implements certain safeguards. These include standard contractual clauses, binding common rules, and certificates of accreditation. In addition, controllers must conduct a risk assessment for such transfers.

- In exceptional cases, transfers are allowed without either adequacy or safeguards. These exceptions include: performing an obligation under an international agreement to which Saudi Arabia is a party, serving the interests of Saudi Arabia, performing an an obligation to which the data subject is a party, performing necessary operations that enable the controller to conduct its activity, providing a service or benefit to the data subject, or conducting scientific research.

- In addition, the controller should inform the data subject of whether their personal data is to be transferred and should conduct a risk assessment for transfers of sensitive data on a continuous and widespread basis.

- The SDAIA has issued several guidelines relating to data transfers, specifically on binding common rules and the standard contractual clauses. The guidelines assist controllers in transferring personal data to countries without appropriate data protection levels.

  Previously – although no longer in force – the Data Sharing Interim Regulations required data storage and processing to occur within the national territory, to preserve digital sovereignty, unless the government provided written approval.

SOURCES

Primary Legislation

- Personal Data Protection Law of 2021 with amendments in 2023

Secondary Legislation

- Saudi Data and AI Authority: Regulation on Personal Data Transfer Outside the Kingdom

Guidelines

- Guidelines for Binding Common Rules (BCR) For Personal Data Transfers
- Guidelines for Standard Contractual Clauses For Personal Data Transfers
- Previous Rules - no longer in force
- The Data Sharing Interim Regulations

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.

Saudi Arabia does not generally require data to be localised. Specific data localisation regimes apply regarding government data, as well as data regarding insurance, accounting, and employer records. Localisation is motivated by the pursuit of digital sovereignty and data protection.

Summary

- Saudi Arabia does not generally require data to be localised but demands localisation for specific data types.

- The KSA Cloud First Policy, which applies to governmental and semi-governmental entities, states that data categorised as classified and top classified must be hosted in "Government Cloud Services."

- Prior to migrating to cloud storage, entities must categorise data into four tiers (open, restricted, classified, top classified), along the Data Classification Policy. While open and restricted data can be stored on "commercial government cloud services", classified and top classified data is only to be stored in local "government cloud services." In addition, the "Data Office" must approve the categorisation.

Sectoral data localisation mandates also apply, namely:

01 The Implementing Regulation of the Income Tax Law requires taxpayers' books to be kept within Saudi Arabia.

02 The Insurance Market Code Of Conduct Regulation requires insurance companies to ensure that personal data is protected by keeping it in Saudi Arabia.

05 Payments between two Saudi parties must be processed within Saudi Arabia.

03 Finally, the Labor Law requires employers to maintain certain records, files, and statements at the workplace.

04 Previously – although no longer in force – the Data Governance Interim Regulations required data to be processed and stored on the national territory, to preserve digital sovereignty, unless the government provided written approval.

SOURCES

Sources

- Primary Legislation
- The Labor Law, 2005

Secondary Legislation

- Insurance Market Code Of Conduct Regulation, 2008
- KSA Cloud First Policy, 2020
- Implementing Regulation of the Income Tax Law, 2004

Oversight Authorities

- The National Data Management Office

- Previous Rules - no longer in force
- The Data Governance Interim Regulations

Online Consumer Protection

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

Guiding Questions

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

Online consumers are protected under the E-Commerce Law. The law prohibits practices, including misleading consumers through misrepresentations, and enables consumers to rescind contracts and receive refunds in view of delays. E-commerce platforms have to uphold transparency requirements regarding their terms and conditions but are not subject to indirect obligations. Spam is regulated by a dedicated regulation, which establishes a general prohibition for spam and requirements for promotional messages to include contact details and an unsubscribe option. The Ministry of Commerce oversees online consumer protection.

Summary

- There is currently no comprehensive consumer protection law in Saudi Arabia, although drafts are being considered. Several legislations govern online consumer protection, such as the E-Commerce Law, enacted in 2019, which includes provisions for products and services sold online. The law applies to providers both inside and outside Saudi Arabia who sell to Saudi consumers.

- Other laws include the Anti-Commercial Fraud Law 2008 and the Commercial Data 2002 which provide consumer protection as well.

  The E-Commerce law and its implementing regulations grants consumers the right to correct an error in communication with the service provider, to terminate the contract, and to after-sale services.

- The consumer may rescind the contract in case of delivery delay for more than 15 days, and demand a refund. Service providers must include information on consumer complaints and must refrain from making misrepresentations that mislead consumers on their "e-shop", as well as register in the commercial register.

- The Ministry of Commerce is responsible for overseeing consumer protection in Saudi Arabia. It issued the Implementing Regulation of the E-Commerce law, the Implementing Regulations of the Commercial data law, and the Guide to Consumer Rights and Responsibilities. It also handles consumer complaints, monitors compliance and provides guidance on consumer rights. A current focus of the Ministry is ensuring safety in direct-to-consumer imports, especially small parcels purchased through social media and other direct-sales channels that pose a particular risk.

Other relevant authorities include:

01 The Saudi Central Bank, which oversees consumer protection within the financial sector and developed the Banking Consumer Protection Principles.

02 The Insurance Commission, which regulates consumer protection issues within the insurance sector and released the Online Insurance Activities Regulation and the Insurance Consumer Protection Principles

03 The Communications and Information Technology Commission, which addresses consumer protection in the telecommunications and ICT sectors.

- In 2018, the Communications, Space and Technology Commission issued the Regulation for Reduction of Spam pursuant to the Telecom Act. The Regulation generally prohibits spam.

- Senders of electronic promotional messages must include contact details and enable recipients to unsubscribe for free and easily. **In addition, the regulation classifies SMS into five types:**
  - Warning messages;
  - Awareness messages;
  - Service messages;
  - Personal messages; and
  - Promotional messages.
  - Telecommunication service providers are to filter promotional messages.

SOURCES

- **Primary Legislation**
- Draft Consumer Protection Law of 2022
- E-Commerce Law of 2019
- Anti-Commercial Fraud Law for the year 2008
- The Law of Commercial Data, 2002 and its amendments
- Telecommunications and Information Technology Act

Secondary Legislation

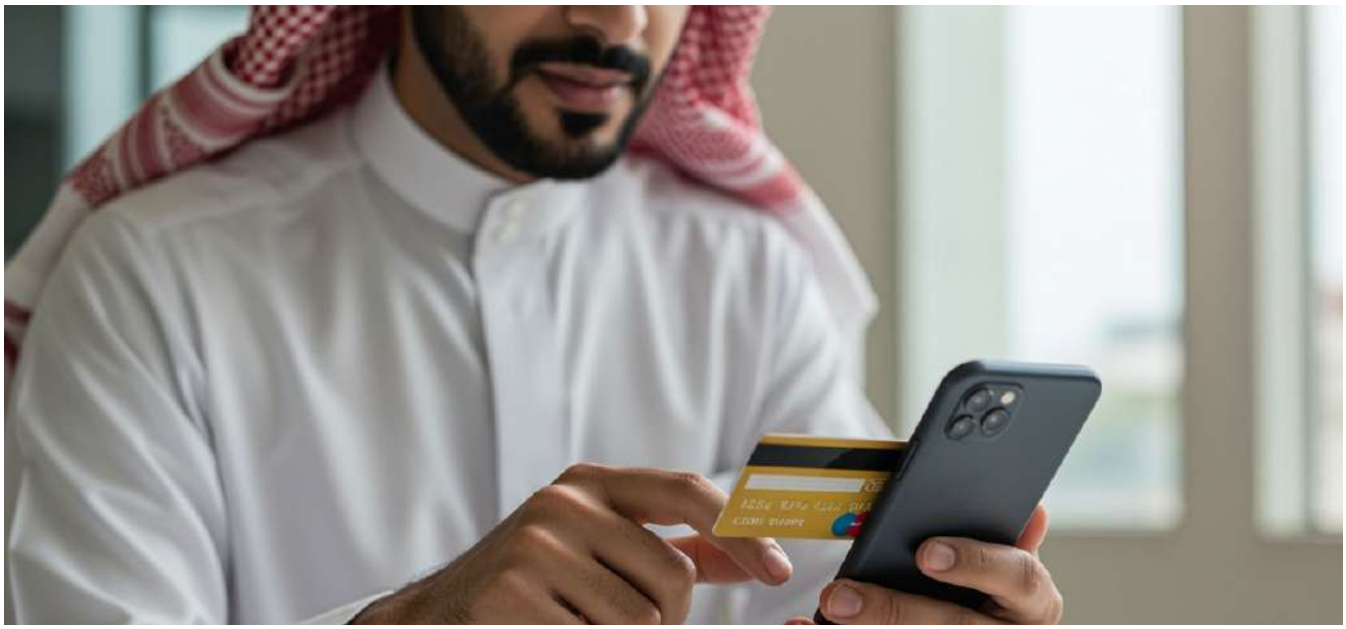
- Regulation for Reduction of Spam, 2018
- Implementing Regulations of the E-Commerce law
- Implementing Regulations of the Commercial data law
- Online Insurance Activities Regulation
- Insurance Consumer Protection Principles
- Financial Consumer Protection Principles and Rules

Guidelines

- Guide to Consumer Rights and Responsibilities 2023

Oversight Authorities

- Ministry of Commerce
- Communications, Space and Technology Commission
- SAMA, Central Bank of Saudi Arabia
- Insurance Authority



Electronic Transactions

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

Guiding Questions

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

Electronic transactions are governed by a dedicated law, which establishes the validity and enforceability of electronic transactions, records, and signatures. Exceptions include transactions related to personal status and real estate. The law does not differentiate between different types of electronic signatures and establishes a mechanism for the government to approve foreign-issued digital certificates.

Finally, the law enables the licensing of digital certification providers for the private sector, while the government's Etimad portal enables authentication related to government services.

Summary

- The Electronic Transactions Law, in force since 2007, provides a legal framework for electronic transactions and signatures. It covers all contracts, with exceptions for transactions pertaining to personal status and real estate, among others. The Law establishes that electronic transactions and records are valid and enforceable. Information resulting from electronic transactions remains in effect as long as it is accessible.

- The Law further establishes that electronic signatures have the same legal effects as hand-written signatures, with certain conditions but without differentiating types of electronic signatures.

- The Law establishes the National Centre for Digital Certification with oversight and the issuance of digital certificates. The Centre has the power to approve digital certificates issued by foreign parties outside of Saudi Arabia and oversees the licensing of certification service providers for digital signatures in the private sector. In addition, the government developed the Etimad portal for authentication related to government services.

- The Electronic Commerce Regulation and its Implementing Instructions mandate the Ministry of Commerce to regulate e-shops, authentication agencies, and platforms which serve as intermediary between consumer and service provider.

- Subsequently, the Ministry of Commerce developed the Guide on Electronic Shops in 2023, which addresses electronic shop owners to facilitate their establishment and operation. In addition, an e-shops compliance self-assessment checklist was developed to assess compliance with requirements.

- FInally, the Zakat, Tax and Customs Authority issued the VAT Guideline for Electronic Contracts, explaining VAT treatment for electronic contracts between providers and buyers.

  The Ministry of Commerce is currently aiming to consolidate fragmented rules under more than 20 authorities into a single, modernised law to govern both online and offline commerce, driven in part by a surge in e-commerce-related consumer complaints.

SOURCES

Primary Legislation

- Electronic Transactions Law, 2007

- **Secondary Legislation**
- Ministry of Commerce: E-commerce Regulation, 2019
- Ministry of Commerce: Implementing Instructions for E-Commerce Regulation, 2020

Guidelines

- Guide on e-shops, 2023
- e-shops compliance self-assessment checklist
- Etimad Portal
- The VAT Guideline for Electronic Contracts

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.

Saudi Arabia provides trade administration documents in electronic form and enables electronic submission. The National Single Window (Fasah) is operational and enables importers, exporters, and freight forwarders to submit shipment declarations and other documentation online. Shipments valued below SAR 1000 are exempted from customs duties.
personal shipments valued below QAR 1000.

Summary

- Saudi Arabia developed a fully operational single window for trade (Fasah) which provides trade administration documents in electronic form and allows importers, exporters, and freight forwarders to submit shipment declarations and other documentation online through Fasah. Shipments valued below SAR 1000 are exempt from customs duties.

- To facilitate reporting and the exchange of data between all parties involved in the clearance of goods, both private and governmental, the Fasah platform connects all the organisations involved in the regulation of trade, such as the commerce and customs authorities.

- The Fasah platform enables trade actors to access 149 import and export services electronically. Importers and Customs brokers can use the Shipment Tracking Service to track the movement of shipments, from their departure to their release from the port of entry, easily and accurately. They also receive notifications of the status of their customs declarations via the system.

- The Saudi Vision 2030 aims to transform the Saudi economy by enhancing trade efficiency and infrastructure. As part of this vision, the government has invested in digital transformation and streamlined trade processes to boost economic diversification and global competitiveness.

  The Vision emphasises modernising customs operations and improving logistical frameworks, aligning with the goals of initiatives like Fasah and the Clearance Within Two Hours Initiative.

- In 2023, the Saudi Zakat, Tax and Customs Authority (ZATCA) launched the Clearance within Two Hours Initiative. This initiative brought together 26 government agencies involved in the clearance process, plus several public and private entities, with the aim of identifying inefficient processes, designing new procedures and implementing new services and IT solutions, while taking into account the competencies of each authority and the nature of its missions.

SOURCES

Primary Legislation

- Electronic Transactions Law, 2007
- The Common Customs Law of the GCC States

Guidelines

- Saudi Vision 2030
- Fasah Portal
- Zakat, Tax and Customs Authority: Threshold exemption from customs duties
- Zakat, Tax and Customs Authority: Clearance within two hours initiative

Cybersecurity

This section aims to assess whether the cybersecurity requirements of the member state broadly align with international best practices. While cybersecurity is a critical component of digital policy, its relevance to digital trade is limited.

Cybersecurity primarily concerns national defence, critical infrastructure, cybercrime prevention, and system integrity. However, alignment with international cybersecurity standards is essential for creating a secure environment conducive to digital trade.

Insufficient cybersecurity standards can undermine trust, while overly stringent requirements may hinder market entry for international service providers.

Guiding Questions

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

Cybersecurity is regulated under the Anti-Cyber Crime Law of 2007. The law establishes several criminal offences in cyberspace and implements a tiered penalty system based on the gravity of offences. Other legal frameworks establish cybersecurity obligations, including incident notification requirements towards authorities. The National Cyber Security Authority is in charge of oversight.

Summary

- The Anti-Cyber Crime Law, enacted in 2007, aims to enhance information security and protect rights pertaining to the legitimate use of computers and information networks. The law identifies cybercrimes and includes provisions on the penalties associated with violations of the law.

- Cybercrimes include, among others, unauthorised access with the intention of cancelling, deleting, destroying, leaking, damaging, altering, or redistributing private data, and causing an information network to halt or breakdown, or destroying, deleting, leaking, damaging, or altering existing or used programs or data.

- The Personal Data Protection Law states that controllers should notify the competent authority and the data subject of data breaches. The Implementing Regulation specifies that such notification is due within 72 hours.

  The National Cybersecurity Authority (NCA), established in 2017 by Royal Order, is the national authority responsible for cybersecurity.

  The NCA is tasked with licensing cybersecurity service providers and developing the cybersecurity controls and standards.

Other relevant authorities include:

01 The Communications, Space and Technology Commission, pursuant to the Anti-Cyber Crime Law, provides assistance and technical support to competent security agencies during the investigation of cyber crimes.

02 The Bureau of Investigation and Public Prosecution carries out the investigation and prosecution of the crimes stipulated in the law.

03 The Saudi Data and AI Authority (SDAIA) receives notifications of data breaches under the the Personal Data Protection Law.

The NCA issued several cybersecurity regulations and guidelines, including:

01 The Essential Cybersecurity Controls Regulations, which applies to all private and public organisations and sets the minimum levels of cybersecurity requirements.

02 The Cloud Cybersecurity Controls Regulations, which impose cybersecurity requirements for cloud service providers and require operators of critical national infrastructure to only use cloud services of licensed providers.

03 The Organisations' Social Media Accounts Cybersecurity Controls, which aim to contribute to raising the level of cybersecurity at the national level, enabling organisations to use

04 social media networks in a safe manner, and respond effectively to cyber incidents.

05 The National Policy for Managed Security Operations Centres (MSOC), which aims to support and improve MSOC services and outlines technical standards regarding cybersecurity.

06 Assessment and compliance tools for both Cloud Service Providers (CSP) and Cloud Service Tenants (CST).

07 The Cyber Security Guidelines for E-Commerce providers and consumers. The Cybersecurity Toolkits and The National Cybersecurity Strategy.

08 Other cybersecurity frameworks, which focus on telework, critical systems, data, and operational technology (see full list below).

- The NCA pursues a multi-level approach that begins with light-touch regulation and escalates only if threats materialize.

- The process evolves from self-regulation or minimal controls to binding, comprehensive rules as threat assessments warrant. By incrementally tightening requirements, the authority maintains flexibility for innovation while

SOURCES

Primary Legislation

- Anti-Cyber Crime Law, 2007
- Personal Data Protection Law of 2021 (amended in 2023)

Secondary Legislation

- National Cybersecurity Authority: Essential Cybersecurity Controls (ECC – 1: 2018)
- National Cybersecurity Authority: Cloud Cybersecurity Controls (CCC – 1: 2020)
- National Cybersecurity Authority: Telework Cybersecurity Controls (TCC)
- National Cybersecurity Authority: Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
- National Cybersecurity Authority: Data Cybersecurity Controls (DCC-1:2022)
- National Cybersecurity Authority: Operational Technology Cybersecurity Controls (OTCC-1:2022)
- National Cybersecurity Authority: Organisations' Social Media Accounts Cybersecurity Controls
- National Cybersecurity Authority: The National Policy for Managed Security Operations Centres
- Saudi Data and AI Authority: The Implementing Regulation of the Personal Data protection Law

Guidelines

- National Cybersecurity Authority: The National Cybersecurity Strategy
- National Cybersecurity Authority: Cybersecurity Guidelines for E-commerce Consumers
- National Cybersecurity Authority: Cybersecurity Guidelines for E-commerce Service Providers
- National Cybersecurity Authority: Cybersecurity Toolkits
- National Cybersecurity Authority: Cloud Service Providers (CSP) Assessment and Compliance Tool
- National Cybersecurity Authority: Cloud Service Tenants (CST) Assessment and Compliance Tool

Oversight Authorities

- National Cybersecurity Authority
- Communications, Space and Technology Commission

Artificial Intelligence

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

Guiding Questions

We outline whether there is a specific regulatory framework addressing AI. If so, we analyse whether the framework is risk-based, meaning it establishes obligations based on the level of AI risk. We also analyse whether the framework is technology-based, meaning it establishes rules based on specific AI technologies. Finally, we reference guidance released by regulatory agencies on how the existing, non-AI-specific framework, applies to AI providers. There is currently no specific binding framework on the governance of AI. As such, neither risk-based nor technology-based requirements apply to AI providers.

The government has focused on enhancing the local AI sector as well as government use of AI in several non-binding policy documents, for example the National Strategy for Data and AI and the Generative AI Guidelines for Government 2024. No regulatory agencies have issued guidelines on how existing rules apply to AI providers.

Summary

There is currently no primary or secondary legislation specifically regulating AI. Saudi Data and AI Authority (SDAIA) is an independent agency that oversees AI in Saudi Arabia, including through its specialised National Centre for AI.

The SDAIA has developed the AI Ethics Principles, which apply to all AI stakeholders designing, developing, deploying, implementing, using, or being affected by AI systems within Saudi Arabia. It covers public entities, private entities, non-profit entities, researchers, public services, institutions, civil society organisations, individuals, workers, and consumers.

The SDAIA carries out the ethics development, developing an adoption plan, advisory, compliance measurement, and compliance monitoring.

In addition, the SDAIA has issued several AI-related frameworks:

01 The SDAIA issued the National Strategy for Data and AI identifying education, government, healthcare, energy, and mobility as priority sectors.

02 The SDAIA issued guidelines on generative AI, specifically regarding education, entertainment, government, and the public.

03 The SDAIA developed the Saudi Academic Framework for AI qualifications, contributing to AI education.

04 The SDAIA and the Ministry of Media launched initiatives to advance AI, specifically the AI Centre for Media and the Future Camp of Generative AI for Media.

Moreover, the Saudi Food and Drug Authority developed the Guidance for AI and Machine Learning-Enabled Medical Devices.

The guidance clarifies the requirements for obtaining Medical Devices Marketing Authorization for medical devices based on AI and machine learning, in order to place them on the market in Saudi Arabia.

SOURCES

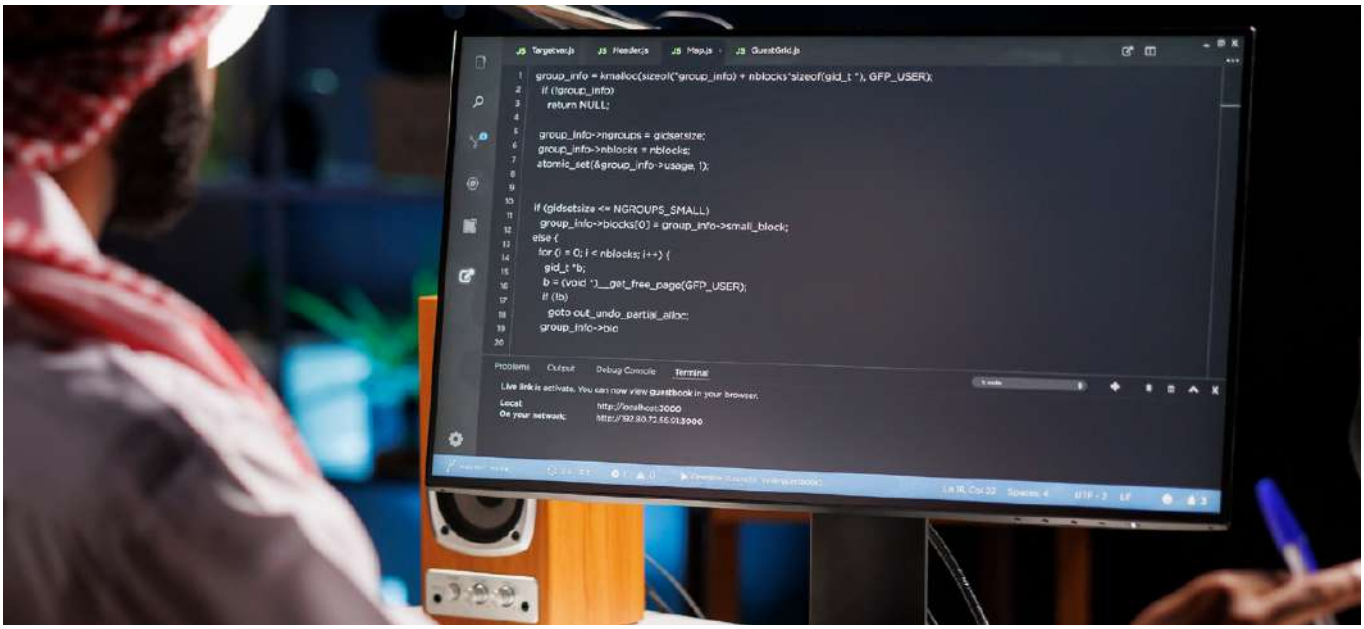
- **Secondary Legislation**
- AI Ethics Principles

Guidelines

- Saudi Data and AI Authority: National Strategy for Data and AI
- Saudi Data and AI Authority: Generative AI Guideline for Government, 2024
- Saudi Data and AI Authority: Generative AI Guideline for Public, 2024
- Saudi Data and AI Authority: The Saudi Academic Framework for AI Qualifications
- Saudi Data and Artificial Intelligence: Generative AI Guide in Education
- Saudi Data and Artificial Intelligence: Generative AI Guideline in Entertainment
- Guidance on Artificial Intelligence (AI) and Machine Learning (ML) technologies based Medical Devices

Oversight Authorities

- Saudi Data and AI Authority
- The National Centre for AI



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 programs as works created in the fields of literature, arts, and sciences, for 50 years from the date of first show or publication. Any use of software contrary to the uses specified by the copyright holder are deemed as infringements of author's rights, including reproduction, and leasing or licensing.

Exceptions to the protection include a permission for possessors of the original copy to make a reserve copy of a consumer program, to protect the original. Saudi Arabia does not mandate any form of source code sharing.

Summary

- The Copyright Law categorises computer programs, software and games, whether in source or machine language, as literary works. Any use of the software to the contrary of the uses specified by the copyright holder is considered an infringement of the right of the author.

- This protection extends to reproduction, leasing and licensing, among others, and lasts for 50 years. Exceptions are foreseen, including making one reserve copy of computer programs by the persons for the purpose of protecting the original.

  Authors have the right to object to the reproduction or sale of their works after the expiration of the protection period, in the event of damage to the author`s honour and reputation, or of distortion of the work.

- Any person who proves a resurrection through websites on the World Wide Web shall be considered an infringer of the right of the author.

  Websites on the World Wide Web shall be responsible for any violation committed to the author's copyright according to the internal content of the site, items broadcasted through it, or through which it is linked to the site by an external link of another subordinate site in the case of a proven violation. The implementing regulation specifies these provisions, including compulsory licensing to reproduce a work or translate a work into Arabic.

- The Saudi Authority for Intellectual Property developed the Guiding Policy on Protecting Copyrights for Software. The guidelines cover the transfer of rights, contractual relationships, the registration of copyrights for computer programs, databases, electronic applications, and digital platforms, as well as procedures for infringement complaints.

SOURCES

Primary Legislation

- The Copyright Law and its amendments

- Secondary Legislation
- Saudi Authority for Intellectual Property: Implementing regulation of Copyright Law

Guidelines

- Guiding Policy on Protecting Copyrights for software

Digital Economy Taxation and Customs Duties

The purpose of this section is to identify how the digital economy is taxed domestically and at the border. This covers direct taxes, indirect taxes, and customs duties, applicable to both digital services/products and e-commerce imports.

We focus on whether a) requirements are applied identically to digital services/products as to their analog equivalents and b) requirements are applied identically to domestic and foreign suppliers.

Guiding Questions

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

Digital services or digital products are not subject to customs duties but are subject to value-added tax. E-commerce imports are subject to both customs duties and value-added tax, although a de minimis threshold of SAR 1000 exempts shipments valued less from customs duties. There are no specific direct taxes on providers of digital services or digital products. Tax registration is mandatory and can be obtained electronically.

Summary

- Customs duties apply to imports, including e-commerce shipments, in line with the Gulf Cooperation Council's Common Customs Law. A duty exemption applies when the total value of purchases is below SAR 1000, including the value of the goods, shipping costs, and insurance.

- The value-added-tax (VAT), regulated by the VAT Law and its Implementing Regulation, is generally 15% and applies to digital services and e-commerce imports. The collection is the responsibility of the service provider.

- For services supplied through an online interface or portal, acting as an intermediary for a non-resident supplier, the operator of the interface or portal is presumed to purchase and subsequently supply the services in their own name. The operator is thus liable to pay tax on any such supply.

- Non-resident service suppliers must register with the tax authority after their first supply of service to a person in Saudi Arabia. Non-resident service providers can appoint a tax representative who will be jointly liable for tax payment. Providers based in Saudi Arabia are obliged to register for VAT if their yearly sales exceed SAR 375,000.

- Saudi Arabia does not impose specific direct taxes on providers of digital services/products. Income Tax Law applies to non-resident providers to residents in Saudi Arabia.

  The Zakat, Tax and Customs Authority developed a Guideline for Taxation of Software Payments which includes different cases of selling software by a non-resident provider to residents in Saudi Arabia and their tax treatment.

SOURCES

Primary Legislation

- Value Added Tax Law for the year 2018
- Common Customs Law of the GCC States
- Unified Agreement for Value Added Tax (VAT) of the Cooperation Council for the Arab States of the Gulf

Secondary Legislation

- Implementing Regulation of the Value Added Tax Law for the year 2016 and its amendments

Guidelines

- Zakat, Tax and Customs Authority: Threshold exemption from customs duties
- VAT Registration Portal
- VAT Guideline for Electronic Contracts
- Guidelines for Taxation of Software Payments in the context of domestic Income Tax Law

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.

Electronic payments are governed by the general regulatory framework for payments, comprising several laws. Know-your-customer, anti-money-laundering, and counter-terroism-financing rules, enshrined in the Anti-Money Laundering Law, apply to electronic payment providers. A licence as Payment Services Provider, issued by the central bank, is required to provide electronic payment services.

Summary

- The Law on Payments and Payment Services was enacted in 2022 and implemented by the Saudi Central Bank. It covers all services related to the execution, transfer, or processing of payment transactions and payment instruments, including e-money payments and payment wallets in the form of electronic accounts or records. The Implementing Regulation of the Law on Payments and Payment Services, enacted in 2023, states that the Saudi Central Bank is responsible for licensing entities to engage in one or more Relevant Payment Services.

- The Anti-Money Laundering (AML) Law and the Law on Combating the Financing of Terrorism (CTF) require financial institutions to know its customers and beneficial owners sufficiently to classify customer and business relationship risks from an AML/CTF perspective to direct its necessary resources to high-risk customers and business relationships to mitigate ML/TF risks.

- To achieve this objective, the financial institution shall classify customers based on the risks associated with them, as mentioned in the ML/TF Risk Assessment Section in this Guide. The information obtained from customers is the main basic tool for classifying customer risks.

- Therefore, the financial institution shall obtain reliable information from customers, verify such information, and ensure that it is updated and appropriate.

- The Anti-Money laundering Permanent Committee, which oversees the implementation of the AML and CFT laws, developed several guidance documents to help financial institutions develop and adopt a risk-based approach for conducting their business in compliance with regulations.

  In addition, the Saudi Central Bank has launched its own payment processing service (MADA) as a cost-effective alternative to major international processors. This critical digital public infrastructure lowers fees for digital payments to foster a robust digital economy.

SOURCES

Sources

- Primary Legislation
- Law of Payments and Payments Services, 2022
- Anti-Money Laundering Law
- Law on Combating the Financing of Terrorism

Secondary Legislation

- Implementing Regulation of the Law of Payments and Payment Services, 2023
- Implementing Regulation to the Anti-Money Laundering Law
- Implementing Regulations of the Law of Combating Terrorist Crimes and its Financing

Guidelines

- The Anti-Money Laundering and CounterTerrorism Financing (AML/CTF) Guide
- Guidelines on Combating Money Laundering and Terrorist Financing

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.
Saudi Arabia has implemented a range of initiatives to support SMEs and disadvantaged groups in digital trade as part of its Vision 2030 strategy. These initiatives span e-commerce, digital payments, technological innovation, and skills development. The government aims to increase the digital economy's contribution to GDP from 13% to 19.2% by 2025 and raise SMEs' contribution to GDP from 20% to 35% by 2030. To achieve these objectives, the Saudi government employs various policy instruments, including financial support through loans and grants, regulatory measures like fee caps to encourage electronic payments, capacity building through training and technical support, infrastructure[2] development via innovation centres and entrepreneurship hubs, and targeted programmes for women entrepreneurs and specific sectors such as manufacturing.

Summary

- The National Transformation Program Delivery Plan 2021-2025 identifies e-commerce as an important driver for SME growth. To support their development, the Saudi Arabian SME Bank offers an E-Commerce Loan scheme providing loans of up to SAR 2.5 million to SMEs for e-commerce activities. Additionally, the Small and Medium Enterprises General Authority (Monsha'at) operates e-commerce programmes and services, offering support for e-commerce setup, digital marketing, and electronic payment solutions.

- In the realm of digital payments, Saudi Payments, a subsidiary of the Saudi Central Bank, has implemented measures to encourage SME adoption of electronic payment systems.
  These include capping interchange fees and imposing a ceiling on card surcharges for SMEs. The Saudi Payments Report 2020 outlines these initiatives aimed at enhancing SME contributions to GDP through increased use of electronic payments.

- The Ministry of Communications and Information Technology (MCIT) has established the Center of Digital Entrepreneurship (CODE) to provide training, technical support, and funding for SME digitalisation.

- MCIT also runs a Women Empowerment Program targeting female entrepreneurs, offering upskilling, business accelerators, and facilitated access to financing, with a focus on the tech sector. MCIT also advocates stakeholder engagement throughout the regulatory process, facilitated by the Istitlaa platform, where proposed regulations are posted for public feedback.

- This process includes proactive outreach to ensure companies are aware of new or changing regulations. Istitlaa also serves as a venue for different regulators to coordinate early, identify overlaps or inconsistencies, and collaborate on shared issues in digital policy. MCIT focuses on inclusion by providing grace periods, regular reviews, sandboxing, and clear notification of rules to foster trust.

- For manufacturing SMEs, the Ministry of Industry & Mineral Resources operates the Future Factories Program. This initiative provides transformation blueprints, training, and financial support to help SMEs adopt advanced technologies in their factories.

SOURCES

Guidelines

- Kingdom of Saudi Arabia: Saudi Vision 2030
- Kingdom of Saudi Arabia: National Transformation Program Delivery Plan 2021 - 2025
- Small & Medium Enterprises Bank: E-Commerce Loan
- General Authority for Small and Medium Enterprises (Monsha'at): E-commerce Program
- General Authority for Small and Medium Enterprises (Monsha'at): Innovation Center
- Saudi Central Bank: Saudi Payments Report 2020
- Ministry of Communications and Information Technology: Center of Digital Entrepreneurship
- Ministry of Communications and Information Technology: Women Empowerment Program in Technology
- Ministry of Industry & Mineral Resources: Future Factories Initiative - National Productivity Program

02 Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Saudi Arabia'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 Saudi Arabia'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 16.86% of Saudi Arabia's imports. The share of advanced technology products in exports was considerably lower at 0.34%, indicating a significant technology trade imbalance.

Figure 1: Digital Delivered Services

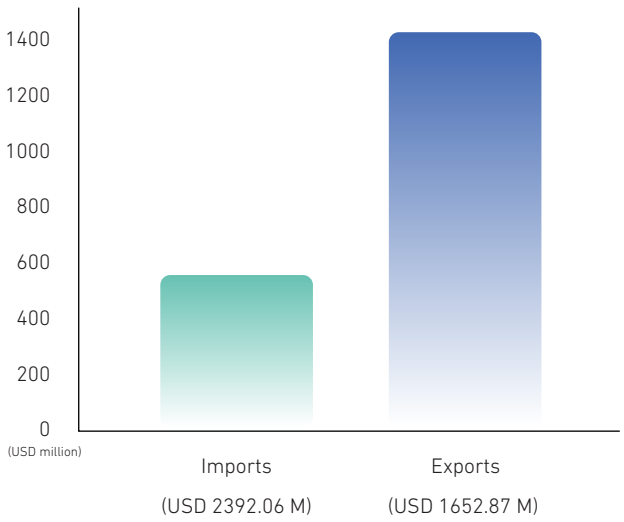


Figure 1 provides data for Saudi Arabia's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

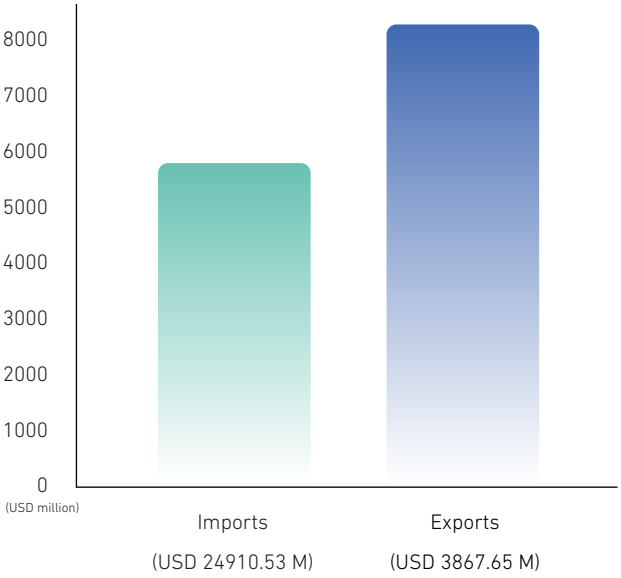


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Saudi Arabia'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

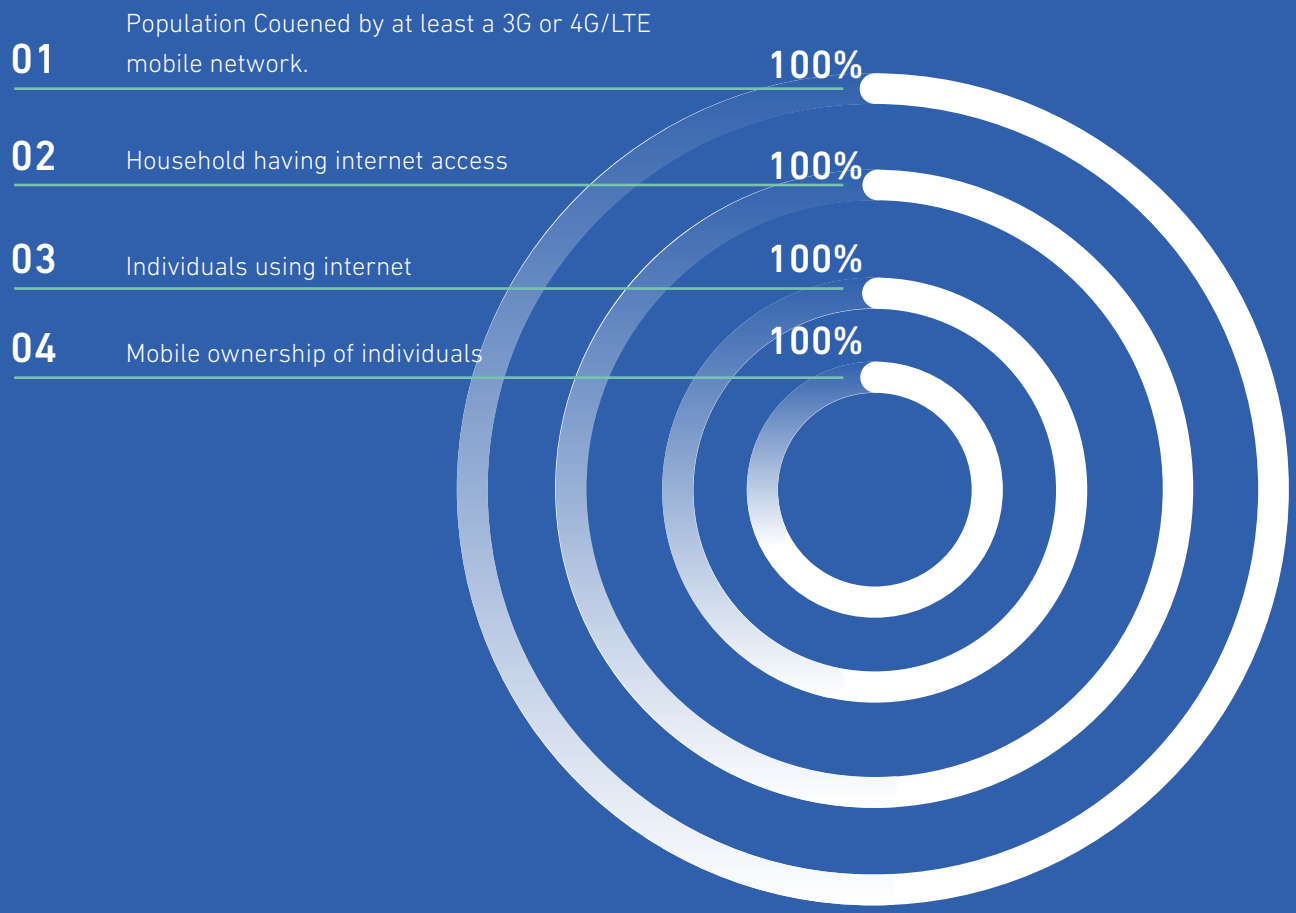


Figure 3 provides data to analyze Saudi Arabia's digital infrastructure and connectivity in 2022.

Digital Skills

To document Saudi Arabia'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 73.75% in 2022, indicating high participation in higher education. The adult literacy rate was 98% in 2020. Government expenditure on education as a percentage of GDP was 4.92% in 2023.

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

- 73.10% were able to copy or move a file or folder (2019).
- 61.70% had created electronic presentations with presentation software (2021).
- 89.50% could find, download, install and configure software (2021).

Digital Government

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

In terms of digital government services in 2022, Saudi Arabia had an operational government cloud platform in use. It had implemented a government interoperability framework. It had a mandatory government open-source software policy. Saudi Arabia maintained both an open government portal and an open data portal.

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

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

01 It had a current government technology or digital transformation strategy

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

03 It had both a strategy and program to improve public sector innovation

03 International Commitments and Collaboration

International Commitments and Collaboration

The purpose of this section is to outline the existing international commitments of the member state and the international fora in which it engages. 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 to which policy area(s) it is pertinent. Regarding international fora, we analyse participation in discussions at the pluri- and multilateral level.

Commitments

Free Trade Agreements

Saudi Arabia 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

Saudi Arabia is party to the following conventions and agreements:

01 United Nations Convention on the Use of Electronic Communications in International Contracts (Electronic Transactions)

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

01 Saudi Arabia is a member state of the United Nations, which has adopted the following frameworks:

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

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

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

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

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

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

08 ESCWA Guideline on personal data protection (Data protection)

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

10 Saudi Arabia is a member of the Group of 20 countries (G20), which has adopted the following frameworks:

11 G20 Artificial Intelligence Principles (G20 Ministerial Statement on Trade and Digital Economy, 2019) (Artificial Intelligence)

12 G20/Organisation for Economic Co-operation and Development High-Level Principles on SME Financing (SMEs and Digital Inclusion)

Models

Saudi Arabia has adopted or been influenced by the following model frameworks:

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

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

Other Commitments

01 Saudi Arabia 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).

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

03 Additionally, Saudi Arabia is a signatory of the following international frameworks:

04 Bletchley Declaration on AI Safety (Artificial Intelligence)

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

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

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

08 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)

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

10 ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity) ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)

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

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

Fora

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

01 United Nations Global Digital Compact (Cross-cutting)

02 Arabian Gulf System for Financial Automated

03 Quick Payment Transfers (Electronic payments)

04 Buna Payment System (Electronic payments)

@dcorg | www.dco.org