
Digital
Cooperation
Organization
Morocco
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:
User consent is generally required before data processing, with exceptions. Data subjects are granted the rights to information, access, rectification, and deletion. Data processors are not obliged to appoint data protection officers or local representation but must notify authorities.

Cross-Border Data Transfers:
Equivalent data protection is required for lawful transfers. The data protection commission maintains a list of countries with such adequate protection. For transfers to other countries, exceptions apply, including data subject consent and single-transfer approval.

Location of Computing Facilities:
Morocco does not have a blanket data localisation mandate but contains four specific mandates covering sensitive data, classified information systems, sectors of "vital importance", and domain name system providers.

Online Consumer Protection:
The consumer protection law explicitly applies online and prohibits practices, such as misrepresentations in advertising. For unsolicited commercial messages (spam) to be lawful, clear information and an effective mechanism to object are required. Automated direct marketing without consent is prohibited under a data protection perspective.

Electronic Transactions:
Electronic transactions hold the same legal standing as paper-based counterparts, as electronic records and evidence cannot be rejected based on their electronic form, with certain exceptions. Simple, advanced, and qualified electronic signatures are differentiated.

Trade Facilitation with Digital Means:

Morocco provides trade administration documents for imports in electronic form and enables electronic submission. The national electronic single window integrates information systems relevant for imports and exports.

Cybersecurity:

Information systems and data types are classified based on the impact of potential cybersecurity incidents. Obligations apply based on this categorisation. Incidents that can affect the security or functioning of systems must be notified to authorities.

Artificial Intelligence:

There is currently no binding framework devoted to the governance of AI. The Ministry of Digital Transition and Administrative Reform is responsible for establishing an AI governance framework and is currently overseeing the implementation of the UNESCO Recommendations on AI, to which Morocco adhered in 2022.

Source Code:

The copyright law protects computer programs as protected works and provides exclusive economic rights to authors, with exceptions for educational and backup purposes. Morocco does not mandate source code sharing.

Digital Economy Taxation and Customs Duties:

Digital services/products are not subject to customs duties but to value-added tax. E-commerce imports are subject to both customs duties and value-added. Morocco has not established a direct tax on providers of digital services/products.

Electronic Payments:

Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payments. Electronic payment providers must obtain a licence from the central bank.

SMEs and Digital Inclusion:

The Moroccan government is currently developing a new strategy for the country's digital transformation and digital economy. Previous such strategies have emphasised the inclusion of SMEs in this process.

01 Domestic Regulatory Environment Assessment

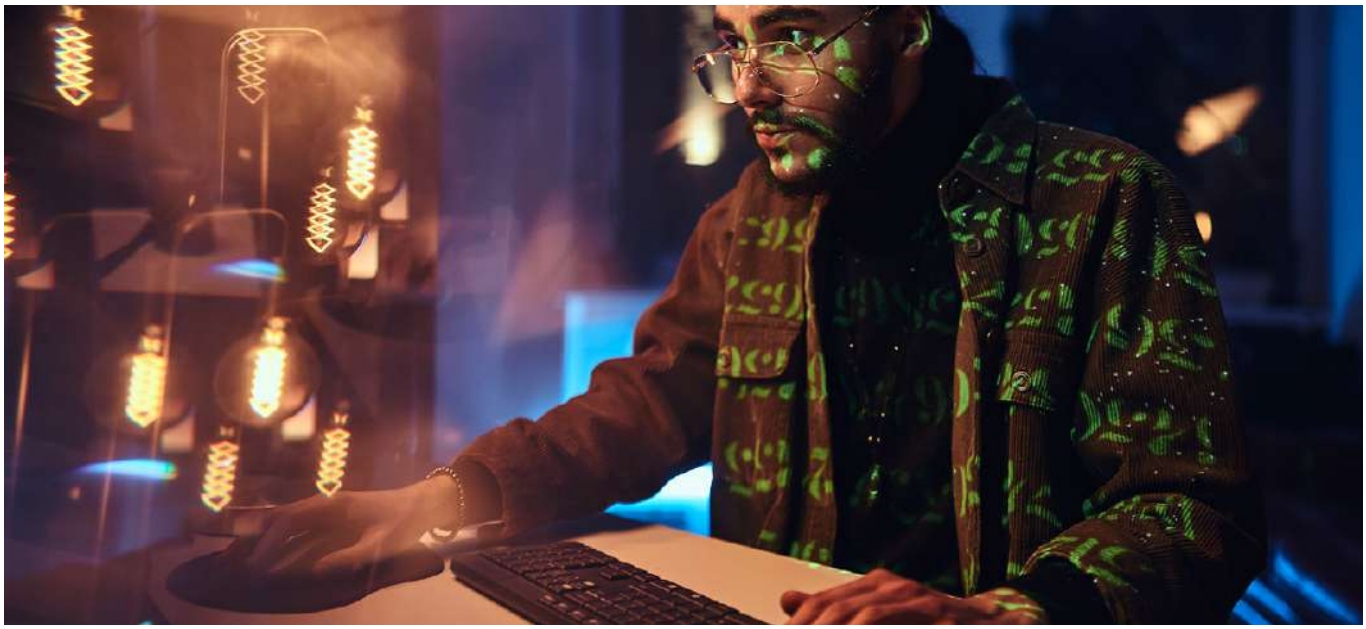
Domestic Regulatory Environment Assessment

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.

User consent is generally required before data processing in Morocco, although there are exceptions such as to execute a contract, fulfil legal obligations, and safeguard vital interests. Data subjects are granted the rights to information, access, rectification, and deletion. Data processors are not obliged to appoint a data protection officer or local representation but have to notify the data protection commission. The commission is in charge of oversight.

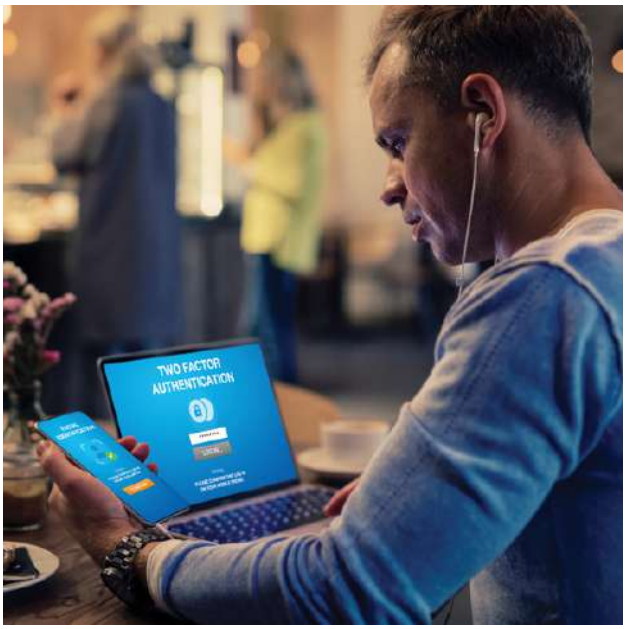
Summary

- The Moroccan Constitution (Chapter 24) recognises the right to confidentiality and privacy of personal communications in all forms and by all means as a right not to be violated. Since 2009, Morocco's primary data protection legislation is the Law on the Protection of Natural Persons with regard to the Processing of Personal Data.

- The law aims at ensuring effective protection of individuals against misuse of their data which could lead to invading their privacy as well as to harmonise the Moroccan system for the protection of personal data with those of its trade partner countries.

- The National Committee to Monitor the Protection of Personal Data (CNDP) is responsible for overseeing data protection in Morocco. The CNDP is an independent body, composed of Moroccan public figures with expertise in data protection, law, and justice. The King appoints the President.

- The CNDP can start investigations, impose sanctions, and draft rules. In 2009, a decree implemented the law and established the CNDP. In 2011, a second decree set the bylaws of the CNDP which includes its organisational structure, roles and responsibilities, as well as the relevant mechanisms and procedures followed in case of violation of the Data Protection Law.



- The CNDP has issued several guidance, publications, and booklets since its establishment. Some are concerned about using workplace surveillance cameras and storing the data, employing biometrics for attendance, and utilising cloud services.

  The three most recent CNDP deliberations are related to a draft directive that sets minimum rules for cloud outsourcing by credit institutions, the use of facial recognition technologies, and the requirements for conducting data protection impact assessments.

SOURCES

Primary Legislation

- Law No. 09-08 (Year 2009) "Law on the Protection of Natural Persons with regard to the Processing of Personal Data Attributes"
- The Constitution of Morocco, Chapter 24.

Secondary Legislation

- Royal Decree 2-09-165 to Establish "The National Control Commission for the Protection of Personal Data"
- Bylaws of the National Committee to Monitor the Protection of Personal Data (CNDP)

Guidelines

- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation D-110-2021 issued on April 30, 2021 providing an opinion on a Draft Directive that sets Minimum Rules for Cloud Outsourcing by Credit Institutions
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation D-195-EUS-2020 issued on December 30, 2020 addressing the use of Facial Recognition Technologies
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation D-188-2020 issued on December 14, 2020, outlines the requirements for conducting Data Protection Impact Assessments (DPIA)
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation No. D-126-EUS-2020 of July 29, 2020 on the definition of the use of Facial Recognition Technologies
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation No. D-120-2020 of 08 July 2020 on the Architecture of Identifiers
- National Committee to Monitor the Protection of Personal Data (CNDP) Deliberation No. D-113-2020 of 22 May 2020 governing the processing of Personal Data in the context of Mail Management
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation N°191-D-AU-2019 of 31 May 2019, on the model application for a Standard Authorisation relating to the Processing of Personal Data
- National Committee to Monitor the Protection of Personal Data (CNDP): Monitoring employees' attendance using Biometric Data
- National Committee to Monitor the Protection of Personal Data (CNDP): Best practices for using the Internet
- National Committee to Monitor the Protection of Personal Data (CNDP): Using Surveillance Cameras in the Workplace
- National Committee to Monitor the Protection of Personal Data (CNDP): Direct promotion of Goods and Services using Email and SMS
- National Committee to Monitor the Protection of Personal Data (CNDP): National Register of Personal Data Protection

Oversight Authorities

- National Committee to Monitor the Protection of Personal Data (CNDP)

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.

Morocco's data protection law establishes dedicated rules for cross-border data transfers, demanding equivalent data protection abroad for lawful transfers. The data protection commission maintains a list of countries with such adequate protection. For transfers to other countries, exceptions apply, including data subject consent, the transfer being necessary for compliance with legal obligations or the protection of vital interests, or the transfer being approved by the data protection commission. Transfers including sensitive data, such as health data, are only allowed after providing the government with information on recipients. Credit institutions are to notify authorities before transferring data to foreign clouds.

Summary

- The Law on the Protection of Natural Persons with regard to Personal Data, enacted in 2009, regulates cross-border data transfers. Data may only be transferred to foreign countries that ensure an adequate level of data protection. The National Committee to Monitor the Protection of Personal Data (CNDP) issued a resolution listing such countries.

- Data transfers to countries not on the CNDP's list are permitted under specific conditions, including the data subject's express consent, derogations (for example the protection of the data subject's life or the preservation of public interest), the execution of an international agreement to which Morocco is party, or based on the CNDP's express authorisation.

- The implementing regulation specifies that, for transfers to non-listed countries, data transfer requests must state specific information, including the name and address of the transferor and recipient, the categories of data being transferred, the individuals concerned, as well as the purpose, mode and frequency of transfers. In addition, requests for transfers based on derogations or international agreements must specify the invoked derogation.

- Finally, requests for transfers based on CNPD approval must indicate the measures taken to uphold data protection, including contractual agreements and internal rules. Finally, transfers including sensitive data, such as health data, are only allowed after providing the CNDP with information on the recipient.

- Finally, the CNDP has issued a deliberation in 2021 establishing a framework for credit institutions to use cloud services based outside of Morocco. Credit institutions using cloud services must notify the CNDP of all personal data processing activities related to cloud outsourcing, including any data transfer requests.

- The eligibility of countries for data hosting should be assessed based on their ability to ensure sufficient protection of personal data. Contracts with cloud service providers must include specific clauses guaranteeing data security and confidentiality, compliance with the data protection law, and must address the transfer of data abroad.

- The contract must also include reversibility clauses, allowing the institution to recover its data at the end of the contract, with specific provisions on data protection and destruction. Institutions are also required to conduct a data protection impact assessment to manage risks associated with the use of cloud services.

SOURCES

Primary Legislation

- Law No. 09-08 (Year 2009) Law on the Protection of Natural Persons with regard to the Processing of Personal Data Attributes

Secondary Legislation

- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation No. D-110-2021 of 30/04/2021 on the opinion on the draft directive laying down the minimum rules for outsourcing to the Cloud
- National Committee to Monitor the Protection of Personal Data (CNDP): Resolution No. 236-2015 of December 18, 2015, amending Resolution No. 465-2013 of September 6, 2013, establishing the list of countries ensuring adequate protection of privacy and the fundamental rights and freedoms of individuals with regard to the processing of personal data

Guidelines

- National Committee to Monitor the Protection of Personal Data (CNDP): Guideline: Data Transfer Abroad
- National Committee to Monitor the Protection of Personal Data (CNDP): Request Form: Data Transfer Abroad
- National Committee to Monitor the Protection of Personal Data (CNDP): CNDP's Countries List
- National Committee to Monitor the Protection of Personal Data (CNDP): Notify a Data Transfer Abroad
- National Committee to Monitor the Protection of Personal Data (CNDP): Guideline: Significant Control Events
- National Committee to Monitor the Protection of Personal Data (CNDP): Standard Information for Data Controllers
- National Committee to Monitor the Protection of Personal Data (CNDP): Conditions of Data Processing
- National Committee to Monitor the Protection of Personal Data (CNDP): Formalities of Data Processing

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.

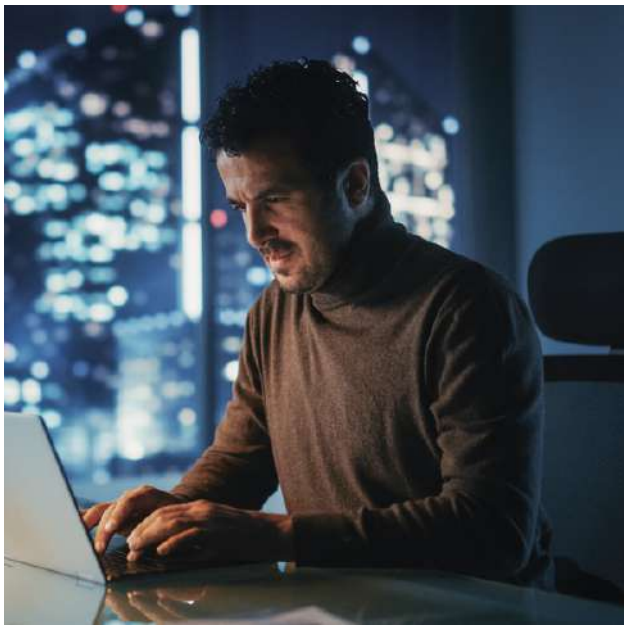
Summary

- Morocco does not generally require data to be stored locally but mandates data localisation for specific categories of data, information systems, and vital sectors (see the cybersecurity section for detailed information on their categorisation).

- The Cybersecurity Law requires "very secret" and "secret" data, the strongest classifications, to be exclusively hosted within Morocco. The implementing regulation of the Cybersecurity Law specifies how information systems are classified, based on the impact of potential cybersecurity incidents.

- Information systems which could cause “very grave impact” and “grave impact” are considered sensitive information systems, implying that they are to be hosted locally. Finally, the cybersecurity law and its implementing decree defines sectors of vital importance and requires providers of such infrastructure to host sensitive data locally.

- Finally, in February 2024, the National Telecommunications Regulatory Agency established a regulatory framework for internet domain names. It establishes technical requirements for service providers, particularly regarding Domain Name System (DNS) hosting.



- Specifically, any entity wishing to provide domain name commercialisation services must possess a secure, continuously operational DNS platform of at least two DNS servers. Crucially, one of the servers must be physically located in Morocco.

SOURCES

Primary Legislation

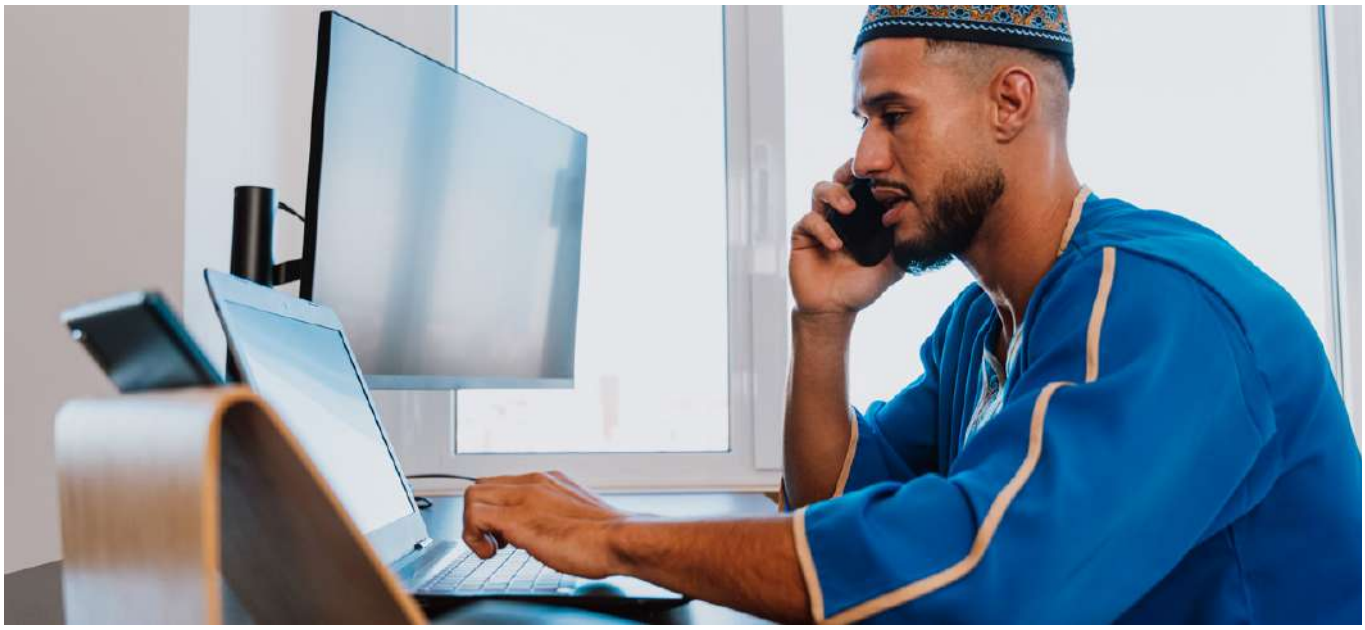
- Law No. 05-20 on Cybersecurity

Secondary Legislation

- Bylaws of the National Committee to Monitor the Protection of Personal Data (CNDP)
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation No. D-110-2021 of 30/04/2021 on the opinion on the draft directive laying down the minimum rules for outsourcing to the Cloud
- National Committee to Monitor the Protection of Personal Data (CNDP): Deliberation D-188-2020 issued on December 14, 2020, outlines the requirements for conducting Data Protection Impact Assessments (DPIA)
- Decree 2-09-165 to Establish "The National Control Commission for the Protection of Personal Data"
- Decree No. 2-21-406 of July 15, 2021 issued for the application of Law no. 05-20 relating to Cybersecurity
- Decree 2-15-712 of February 06, 2016 laying down the system for the protection of sensitive information systems of vital infrastructures
- Decree No. 2-21-406 of July 15, 2021 taken for the application of Law No. 05-20 on Cybersecurity
- Decision ANRT/DG/N°02/2024 of 5 February 2024, on the administrative, technical and commercial management procedures of Internet domain names managed by the ANRT

Guidelines

- General Directorate of Security of Information Systems (DGSSI): Declaration Form: Sensitive Information Systems
- General Directorate of Security of Information Systems (DGSSI): Homologation of Sensitive Information Systems for Vital Infrastructure
- General Directorate of Security of Information Systems (DGSSI): Presentation on Declaration of Sensitive Information Systems of Vital Infrastructures
- General Directorate of Security of Information Systems (DGSSI): Presentation on Directive of National Information Systems Security
- General Directorate of Security of Information Systems (DGSSI): Directive of National Information Systems Security
- General Directorate of Security of Information Systems (DGSSI): DGSSI Presentation on Vital Sectors
- General Directorate of Security of Information Systems (DGSSI): Forms
- National Committee to Monitor the Protection of Personal Data (CNDP): Processing of Personal Data in Morocco
- National Committee to Monitor the Protection of Personal Data (CNDP): Conditions and Obligation
- National Committee to Monitor the Protection of Personal Data (CNDP): Formalities



Online Consumer Protection

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

Guiding Questions

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

The general consumer protection law explicitly applies to the electronic provision of products or services. The law prohibits practices including misrepresentations in advertising and the failure to deliver products or services after charging consumers. E-commerce platforms are not subjected to special obligations and suppliers are responsible for upholding consumer rights even if intermediary services are involved. The law also regulates spam, demanding clear information and an effective mechanism to object to such marketing. In addition, automated direct marketing without consent is prohibited under a data protection perspective. Finally, oversight is divided between the Consumer Protection Division under the Ministry of Industry, Trade, Investment and the Digital Economy, the National Defence Administration's General Directorate of Security of Information Systems, the National Telecommunications Regulatory Agency, and the central bank.

Summary

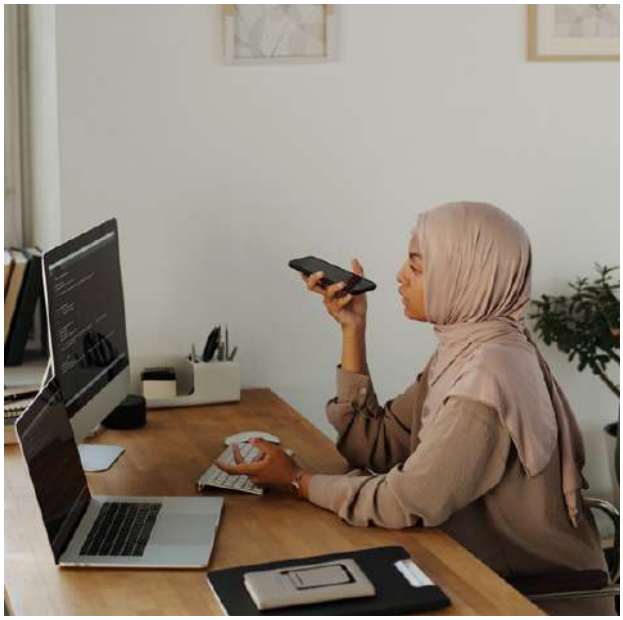
- The Consumer Protection Law of 2011 is the principal legislation addressing consumer protection, including protections related to internet transactions. The law aims to enhance consumer rights, safeguarding against unfair practices, and improving provisions for contractual warranties, and after-sales service.

- The law grants consumers the right to information, right to choose, right to withdraw or return, the right to representation, and the right to protect economic interests. Additionally, two separate laws concerning the standard quality of goods and services, and regulating competition and freedom of prices complement the Consumer Protection Law.

- This supplementary law applies across all sectors of the Moroccan economy with the exception of food and groceries, medicine and medical supplies, and real estate.

- E-Commerce suppliers are responsible for upholding consumer rights, unless that they may be exonerated from all or part of their liability by proving that the non-performance or poor performance of the contract is attributable either to the consumer, or to the unforeseeable and insurmountable act of a third party to the contract, or to a case of force majeure.

- There are multiple decrees and decisions on consumer protection in Morocco. These include the decree issued in February 2011 to implement the Consumer Protection Law, the decision related to the restructuring of the Ministry of Industry, Trade,



- Investment and the Digital Economy to include the Consumer Protection Division, and the decision regulating consumer protection associations. The Consumer Protection Division under the Ministry of Industry, Trade, Investment and the Digital Economy is the main entity responsible for overseeing the consumer protection legislations in view of the quality of the supply of goods and services.

- The division is tasked with conducting inspections, particularly concerning business practices in the trade and industry sectors. The department operates a control unit dedicated to monitoring merchant websites, ensuring that advertisements comply with the provisions of the law.

- The MIT has issued multiple guidelines including on filing complaints through the consumer protection windows spread all over the country, finding the nearest consumer protection association to citizens, and other brochures and booklets related to advertising, online shopping, products labelling, and after-sales services.

- The National Defence Administration's General Directorate of Security of Information Systems (DGSSI) oversees aspects related to online consumer protection.

- It is responsible for consumer safety especially when carrying out online transactions and enforces aspects of e-commerce such as the safety of e-payment platforms and the accuracy of specifications published on the suppliers websites. The DGSSI has issued guidelines addressing safe use and payments on the internet.

- The National Telecommunications Regulatory Agency (ANRT) is responsible for the oversight of telecommunications consumers. The ANRT starts investigations and issues fines in the case of consumer law breaches, contracts issues, and misleading advertisements. The ANRT's most recent guideline, published in 2023, focuses on the telecommunications sector development.

- Furthermore, the Central Bank, Bank Al-Maghrib (BAM) includes a Consumer Protection Department which oversees banking, finance, insurance, and credit institutions. The BAM recently outlined its consumer protection function in a presentation and

- issued specific directives to enhance these protections, such as ensuring clear communication of banking conditions, establishing rules for interest rates and account management.

SOURCES

Primary Legislation

- Law No. 08-31 establishing measures for Consumer Protection, including consumer protection on the Internet
- Law No. 104.12 on Freedom of Prices and Competition [source not working]
- Law No. 12-06 on Standardisation, Certification and Accreditation

Secondary Legislation

- Decree No. 2.12.462 issued on November 14, 2012 defining the Model Statute of Consumer Protection Associations for which the Public-benefit Status [source not working]
- Decree No. 2-12-503 issued on September 11, 2013 adopted for the application of certain provisions of Law No. 31-08 enacting Consumer Protection Measures
- Decree No. 1.11.03 issued on February 18, 2011 implementing Law No. 31.08 establishing measures to Protect the Consumer [source not working]
- Decree No. 2.14.652 issued on December 1, 2014 implementing Law No. 104.12 on Freedom of Prices and Competition [source not working]
- Minister of Industry, Trade, Investment and Economy: Decision No. 2.14 issued on January 2, 2014 concerns researching and proving violations of the provisions of Law No. 31.08 establishing measures to Protect the Consumer [source not working]
- Minister of Industry, Trade, Investment and Economy: Decree No. 05-14 laying down the standard model to which documents, advertisements and regulations presenting the advertising lottery operation for goods, products and services relating to the trade and industry sector must comply with
- Minister of Industry, Trade, Investment and Economy: Decision No. 2041.10 issued on July 7, 2010 with the restructuring of the departments and central directorates of the Ministry [source not working]
- Minister of Industry, Trade, Investment and Economy: Decision No. 1679.14 issued on May 12 2014 concerning the methodology to implement the obligations associated with the safety of products and services [source not working]
- Minister of Industry, Trade, Investment and Economy: Decision No. 07.14 issued on January 2, 2014 determining the standards of the contracts concluded between the suppliers and consumers of goods and services related to contractual guarantee or after-sales service or both with respect to certain goods or products or services in the trade and industry sector [source not working]
- Minister of Industry, Trade, Investment and the Digital Economy and the Minister of Economy and Finance: Joint Decree No. 4030-14 fixing the characteristics and statements of the response slip to the changes proposed by the lender when renewing the credit agreement
- Minister of Industry, Trade, Investment and the Digital Economy and the Minister of Economy and Finance: Joint Decree No. 4031-14 laying down the standard models of prior credit offers and their detachable withdrawal forms
- Minister of Industry, Trade, Investment and the Digital Economy and the Minister of Economy and Finance: Joint Decree No. 4032-14 fixing the maximum default interest rate applicable to the amounts remaining due in the event of the borrower's default
- Minister of Industry, Trade, Investment and the Digital Economy: Decree No. 07-14 laying down the standard model of the writings concluded

SOURCES

between supplier and consumer and relating to the conventional guarantee and/or after-sales service for certain goods, products or services in the trade and industry sector

- Minister of Industry, Trade, Investment and the Digital Economy: Decree No. 3-14 fixing the particulars of the detachable form intended to facilitate the exercise of the right of withdrawal in terms of canvassing in the trade and industry sector
- Minister of Industry, Trade, Investment and the Digital Economy: Decree No. 2-14 on investigators under the Minister of Industry, Trade, Investment and the Digital Economy, responsible for the investigation and finding of infringements of the provisions of Law 31-08
- Minister of Industry, Trade, Investment and the Digital Economy: Decree No. 4-14 fixing the maximum value of small objects or services of low value and samples subject to a premium granted to consumers for goods and products in the trade and industry sector
- Decision of the Minister Delegate to the Prime Minister in charge of Economic and Public Affairs No. 649.07 issued on May 4, 2007 determining the methods of advertising and informing the consumer in the field of telecommunication services

Guidelines

- Consumer Protection Division: All Consumer Protection Windows in Morocco
- Consumer Protection Division: Consumer Protection Associations of Morocco
- Consumer Protection Division: Brochure - The Role of Consumer Protection Associations
- Consumer Protection Division: Presentation of Consumer Protection Associations
- Consumer Protection Division: Updated List - Consumer Protection Associations
- Consumer Protection Division: Updated List - Consumer Protection Windows
- Consumer Protection Division: Filing a Complaint
- Consumer Protection Division: National Consumer Day Reports
- Consumer Protection Division: Consumer Associations at your service
- Consumer Protection Division: The right of withdrawal after purchase
- Consumer Protection Division: Points to check before buying
- Consumer Protection Division: Buy on the internet with confidence
- Consumer Protection Division: Product labelling
- Consumer Protection Division: The guarantee of products and services
- Consumer Protection Division: Poster relating to the portal
- Consumer Protection Division: Poster relating to consumer credit
- Consumer Protection Division: Model General Conditions of Sale for cyber merchants
- Consumer Protection Division: Guide "The purchase of movable property and services"
- Consumer Protection Division: Consumer Protection Associations
- Consumer Protection Division: Abuse of weakness

SOURCES

- Consumer Protection Division: Advertising lottery
- Consumer Protection Division: Sale and service with premiums
- Consumer Protection Division: Product warranty
- Consumer Protection Division: Introductory manual: Education of young consumers
- Consumer Protection Division: Education for young consumers
- Consumer Protection Division: Consumer guide
- Consumer Protection Division: Distance selling
- Consumer Protection Division: Consumer information
- Consumer Protection Division: Display of prices
- Ministry of Industry, Trade, Investment and the Digital Economy: National Consumer Days Presentation [source not working]
- National Telecommunications Regulatory Agency (ANRT): Memorandum of General Directions to continue the development of the Telecommunications Sector of 2023
- Bank Al-Maghrib (BAM): Presentation on Customer protection of credit institutions

Oversight Authorities

- National Telecommunications Regulatory Agency (ANRT)
- Ministry of Industry, Trade, Investment and the Digital Economy [source not working]
- Consumer Protection Division under the Ministry of Trade, Investment and Digital Economy (Khidmat Almostahlik)
- Consumer Protection Observatory
- General Directorate of Security of Information Systems (DGSSI)
- Bank Al-Maghrib

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.

Morocco's binding framework for electronic transactions is enshrined in the Law on Trust Services for Electronic Transactions. Electronic transactions hold the same legal standing as paper-based counterparts, as electronic records and evidence cannot be rejected based on their electronic form. Exceptions are foreseen for documents with specific formal requirements such as notarial deeds and public contracts. The framework differentiates simple, advanced, and qualified electronic signatures. Electronic authentication is accepted but not directly provided by the government.

Summary

- Morocco has established a comprehensive legal framework for electronic transactions through the Law on Trust Services for Electronic Transactions in December 2020. This law provides the foundation to conduct electronic transactions, covering key aspects such as electronic signatures, seals, time stamping, registered delivery services, and website authentication. It ensures that electronic transactions are legally valid and enforceable, promoting their widespread adoption across various sectors.

- To enforce this law, a decree was issued in November 2022, which defines specific rules for each trust service, referencing international standards. The decree outlines procedures for the approval and declaration of trusted service providers and specifies the data required in qualified certificates for e-signatures, stamps, and website authentication.

- Additionally, the decree sets basic rules for electronic registered mail and details the process for issuing, renewing, and suspending certificates of conformity for devices used in electronic signatures or stamps.

  It promotes a trusted third-party ecosystem, encouraging innovation by defining the process for the approval of public sector certification organisations, and outlines the reporting requirements for non-qualified trusted services. Cryptological means and services are also regulated, distinguishing between prior declaration and authorisation regimes, and listing exemptions from formalities.

- In accordance with the law, the legal effect and admissibility as evidence in court of electronic signatures, electronic stamps, electronic time stamps, and electronic registered mail cannot be denied on the sole grounds that they are in electronic form or that they are not qualified. If the electronic signature process is not qualified, then its reliability will have to be demonstrated. For the qualified level, **the law specifies the following legal effects:**

01. The qualified electronic signature has a legal effect similar to that of a handwritten signature in terms of presumption of reliability, without the need for proof of the signature's reliability.
02. The legal effect of a qualified electronic signature combined with a qualified electronic time stamp is equivalent to that of a legalised handwritten signature.
03. The qualified electronic seal benefits from a presumption of data integrity and accuracy of the origin of the data to which it is linked.
04. The law on electronic transactions recognises three levels of electronic signatures, each with specific requirements and legal standing.
05. The “Simple Electronic Signature” does not require any specified technical or functional requirements and is primarily used for simplified transactions. However, it does not benefit from a presumption of reliability, and the burden of proof is on the defendant to demonstrate its authenticity.

06 The "Advanced Electronic Signature" enjoys better legal recognition and involves intermediate technical and organisational requirements, such as the use of an electronic certificate. While it offers greater flexibility for medium-level uses, it still lacks the presumption of reliability, requiring the defendant to prove its authenticity.

07 The "Qualified Electronic Signature" requires the mandatory use of cryptographic products and a qualified electronic certificate, benefiting from a presumption of reliability and legal standing similar to that of a handwritten signature. Electronic authentication, or digital identity management, is also recognised under this framework. The law allows for the issuance of qualified electronic certificates for trust services, with the verification of identity either conducted in-person or remotely. Remote verification must ensure that the means of identification used are authentic and belong to the individual in question, with methods such as CNIE 2 or any official identity document used for this purpose.

- In the presentation of the law, Morocco recognises e-authentication and gives examples of the European Union's eIDAS (Electronic Identification and Trust Services) as one of the main frameworks it has looked upon as it has secured electronic interactions between citizens, businesses, and public authorities through a multitude of trust services. Furthermore, the legislation specifies that to issue a qualified electronic certificate for a trust service, the identity and all attributes of the natural or legal person to whom the certificate is issued must be verified.

- **This verification must be carried out :**
  In person (by the natural person or the authorised representative of the legal entity);
  At a distance, using electronic means of identification whose issuance required the physical presence of the natural person or the authorised representative of the legal entity in front of the entity that issued the means.

- The law also distinguishes between "accredited" and "non-accredited" trust service providers. "Accredited" providers, offering qualified services, are subject to strict regulations and must obtain certification from the national authority before they can operate. "Non-accredited" providers, on the other hand, need only submit a prior declaration to the authority. Both types of providers are held liable for professional negligence or inadequacies, and they are required to maintain records related to the provision of trust services, including notifying the national authority of any security incidents.

- The General Directorate for Information Systems Security (DGSSI) is the designated national authority for trusted services related to electronic transactions. Qualified trust services are subject to stricter requirements, including the of certified devices, regular security audits, and compliance with specific norms and standards.

  The DGSSI has also issued the Frequently Asked Questions about Law on Trust Services on Electronic Transactions guideline, which aims at informing users of the provisions of this text to promote a general and unified understanding among all stakeholders.

SOURCES

Primary Legislation

- Law No. 43-20 relating to trust services for electronic transactions

- Secondary Legislation
- Decree No. 2-22-687 of November 16, 2022 taken for the application of Law No. 43-20 relating to trust services for electronic transactions

Guidelines

- General Directorate of Information Systems Security (DGSSI): Frequently Asked Questions about Law 20-43 on Trust Services on Electronic Transactions

Oversight Authorities

- General Directorate of Information Systems Security (DGSSI)

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.

Morocco provides trade administration documents for imports in electronic form and enables electronic submission. The national electronic single window (PortNet) integrates information systems relevant for imports and exports. It is operational and enables customs clearance and tracking. Finally, as of 2022, there is no expedited procedure for low-value shipments. The previous de minimis threshold of MAD 1250 for e-commerce import shipments was eliminated.

Summary

- In Morocco, paperless trade is regulated primarily by the Customs Code, the Law on Electronic Exchange of Data, and the Law on Trust Services for Electronic Transactions. Import declarations and related documents can be digitised and submitted electronically through the customs administration's system, authenticated with certified electronic signatures.

  In case of system outages, paper submissions are temporarily accepted, but electronic resubmission is required once the system is restored.

- Morocco introduced the PortNet system in 2008, an electronic Single Window that integrates various stakeholders in foreign trade, streamlining import and export procedures. PortNet interconnected software tools with the Automated Base for Networked Customs (BADR) customs clearance system which enable mobile working for customs officers, effective risk management through data collection and analysis, and digital channels for submitting complaints and requests for information.

- These tools also provide economic operators with real-time monitoring of their customs activities and operations via the "Diw@nati" platform.

  As of 2019, the entire customs clearance process became fully paperless, promoting efficiency and reducing the need for physical interaction with customs officials. Currently, economic operators have access to a range of digitised services, including the filing of customs declarations, the option to establish an estimate of duties and taxes,

- consultation of the integrated tariff, the issuing of the customs duty assessment document, the electronic payment of duties and taxes, the issuing of the payment receipt, and the certificate of discharge, enabling banks to release operators from liabilities up to the discharged value. Furthermore, through this system, operators can track the progress of their declarations in real-time.

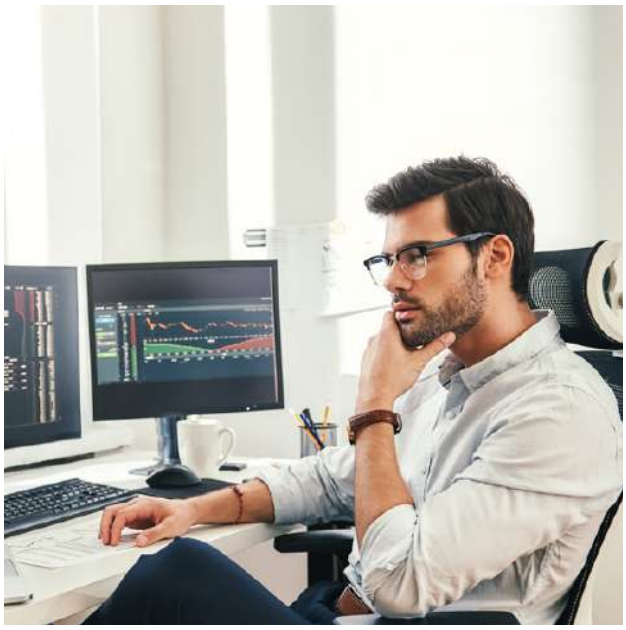
  Morocco has also introduced multi-channel payment solutions allowing customers to settle their customs debts through various secure methods, including online banking. It is also worth noting that banks now input bank security directly into the BADR system, eliminating the need for physical documents.

  BADR is also a transactional system intended for all stakeholders in the customs clearance logistics chain and directly or indirectly concerns a range of foreign trade actors, including importers, exporters, and carriers, among others.

consultation of the integrated tariff, the issuing of the customs duty assessment document, the electronic payment of duties and taxes, the issuing of the payment receipt, and the certificate of discharge, enabling banks to release operators from liabilities up to the discharged value. Furthermore, through this system, operators can track the progress of their declarations in real-time.

Morocco has also introduced multi-channel payment solutions allowing customers to settle their customs debts through various secure methods, including online banking. It is also worth noting that banks now input bank security directly into the BADR system, eliminating the need for physical documents. [1]

BADR is also a transactional system intended for all stakeholders in the customs clearance logistics chain and directly or indirectly concerns a range of foreign trade actors, including importers, exporters, and carriers, among others.



As of 2022, there is no expedited procedure for low-value e-commerce shipments, with customs duties and VAT applying also for goods valued up to MAD 1250.

Furthermore, an assistance system (ADIL) provides full details of the duties and taxes payable, both under preferential regimes and ordinary law, and information about specific regulations for imports and exports.

Finally, the Moroccan Customs and Excise Administration strategic plan for 2024-2028 is structured around seven strategic objectives: supporting national economic policy through improved business climate and competitiveness; adapting customs taxation and enhancing revenue mobilisation; consolidating digital transformation; protecting the economy and business competitiveness through strengthened enforcement against fraud; combating illicit trafficking and ensuring citizen protection; enhancing internal governance and service quality; and strengthening internal capacities through staff training and development.
Key initiatives include revising the Customs and

SOURCES

Primary Legislation

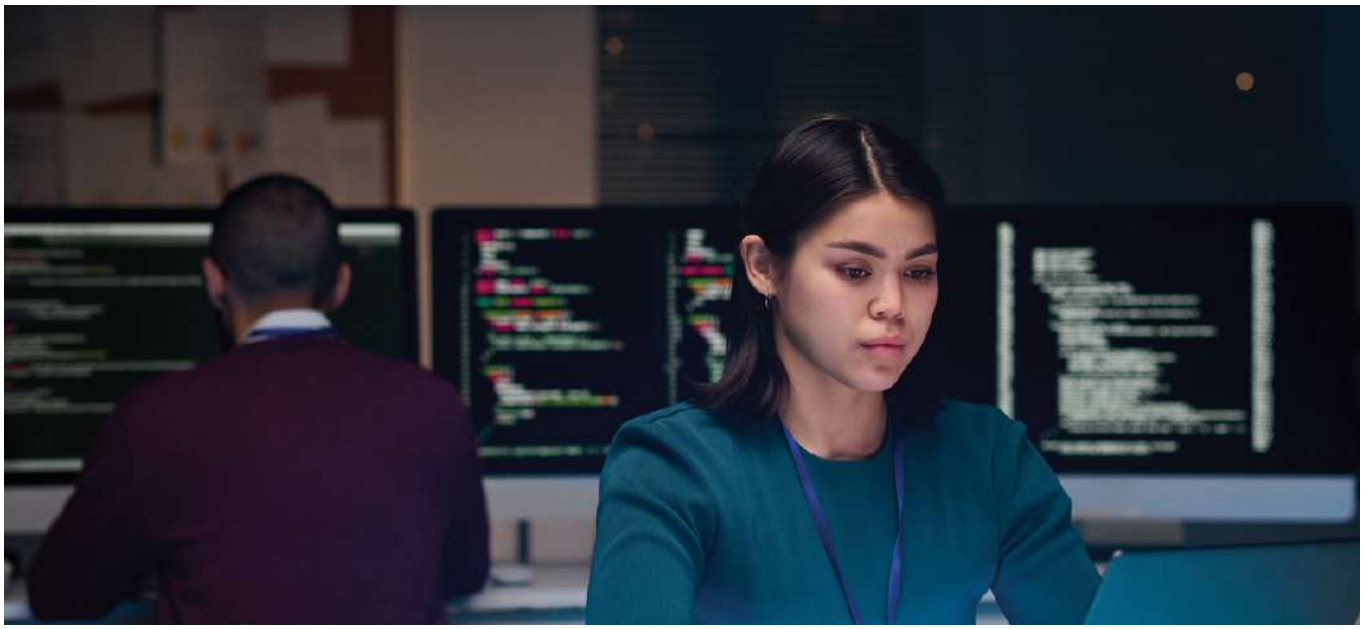
- The Customs Code as of 2024
- Code of Customs and Indirect Taxes approved by Law No. 1.77.339 of October 9, 1977 and it was amended under Law No. 99.02 ratified by the Decree No. 1-00-222 on June 5, 2000
- Law No. 53-05 on the Electronic Exchange of Legal Data
- Index of the Code of Customs and Indirect Taxes

Secondary Legislation

- Decree No. 2-08-518 of May 21, 2009 adopted for the application of Articles 13, 14, 15, 21 and 23 of Law No. 53-05 on the electronic exchange of legal data
- Decree No. 2-13-881 of January 20, 2015 amending and supplementing Decree No. 2-08-518 of May 21, 2009 taken for the application of Articles 13, 14, 15, 21 and 23 of Law No. 53-05 on the electronic exchange of legal data
- Decision of the Minister of Economy and Finance No. 09-1000 issued on April 10, 2009 defining the tariff for products and services provided by the Customs and Indirect Taxes Department
- Decision of the Minister of Economy and Finance No. 11-690 issued on July 22, 2011 determining the types of acceptable economic customer status and the rule of granting this status
- Decision of the Minister of Economy and Finance No. 11-691 issued on July 22, 2011 determining the composition and conditions of the work of the committee tasked with studying applications for the status of an acceptable economic agent
- Decision of the Minister of Economy and Finance No. 16-3176 issued on June 12, 2017 specifying the documents constituting the file of granting advance decisions as well as the methods of granting these decisions

Guidelines

- Ministry of Economy and Finance: eServices Presentation [source not working]
- Presentation of the Customs Code and Indirect Taxes
- Customs Administration: Presentation of Customs in the 21st Century
- Presentation of PortNET
- PortNET User Guides
- PortNET Videos Library
- Presentation of Adil
- Presentation of BADR and RED
- Diw@nati Portal
- Morocco Customs Strategy 2024-2028 [source not working]
- Presentation on the single window: PortNet
- Publications of the Moroccan Customs



Cybersecurity

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

Guiding Questions

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

The cybersecurity law establishes a classification of information systems and data types, based on the impact of potential cybersecurity incidents. Obligations apply based on this categorisation, as well as for providers active in specific "vital sectors." All providers are required to notify government authorities once they are aware of incidents that can affect the security or functioning of systems. The General Directorate of Security of Information Systems is in charge of oversight.

Summary

- In 2003, Morocco introduced its first major legislation related to cybersecurity, amending the penal code to address crimes involving automated data processing systems and penalising unauthorised intrusions. In 2020, Morocco enacted the Cybersecurity Law to establish security rules and protect infrastructure of vital importance that contains sensitive information systems.

  To this end, it classifies information systems and government data into four classes, respectively and establishes proportional obligations, including incident reporting, cybersecurity audits, security approval before operation, and designating a responsible cybersecurity officer.

Information Systems are classified into four classes:

- Class A: If at least one cybersecurity incident affecting the confidentiality, availability, or integrity of any information asset that makes up the information system has a very grave impact.

- Class B: If all cybersecurity incidents affecting the confidentiality, availability, or integrity of the information assets that make up the system have, at most, a grave impact.

- Class C: If all cybersecurity incidents affecting the confidentiality, availability, or integrity of the information assets that make up the system have, at most, a moderate impact.

- Class D: If all cybersecurity incidents affecting the confidentiality, availability, or integrity of the information assets that make up the system have, at most, a limited impact.

- **Similarly, data is classified into four categories:**
  Very Secret: If a cybersecurity incident affecting confidentiality has a very grave impact.

- Secret: If a cybersecurity incident affecting confidentiality has a grave impact.

- Confidential: If a cybersecurity incident affecting confidentiality has a moderate impact.

- Restricted: If a cybersecurity incident affecting confidentiality has a limited impact.

- The law further sets obligations for entities in vital sectors. Morocco issued decrees listing sectors of activity of vital importance.

  As of 2021, **the following sectors were listed:**

01. Public Safety, regulated by the Ministry of Interior
02. Foreign Affairs, regulated by the Ministry of Foreign Affairs, African Cooperation, and Moroccan Expatriates
03. Finance, regulated by the Ministry of Economy and Finance
04. Legislation, regulated by the General Secretariat of the Government

05 Agriculture, regulated by the Ministry of Agriculture

06 Health, regulated by the Ministry of Health Industry, Commerce, and Digital Economy, regulated by the Ministry of Industry, Trade, Investment and the Digital Economy

07 Communications, regulated by the Minister of Youth, Culture, and Communication

08 Energy, regulated by the Ministry of Interior and the Ministry of Energy Transition and Sustainable Development

09 Mining, regulated by the Ministry of Energy Transition and Sustainable Development

10 Transportation, regulated by the Ministry of Transport and Logistics

11 Water, regulated by the Ministry of Equipment and Water

12 Banking, regulated by Bank Al-Maghrib [the central bank]

13 Telecommunications, regulated by the National Telecommunications Regulatory Agency (ANRT)

14 Insurance, regulated by the Supervisory Authority of Insurance and Social Welfare (ACAPS)

15

16

- Three bodies are responsible for overseeing cybersecurity in Morocco. The General Directorate of Security of Information Systems (DGSSI), a government agency, encompasses four directorates:

  The Directorate for the Management of the Vigilance and Incident Response Center (MaCERT), which handles incident monitoring and response.

  The Directorate of Strategy and Regulation responsible for developing the national strategies and proposing legal and regulatory texts.

- The Directorate of Assistance, Training, Control, and Expertise which offers technical recommendations and conducts security audits.

- The Directorate of Secure Information Systems, which develops secure network systems and performs research.

- The Serious Cybercrises and Events Management Committee, chaired by the DGSSI, ensures a coordinated approach to managing cybersecurity incidents and crises. The Strategic Committee for Cybersecurity, an advisory body, formulates cybersecurity strategies, evaluates DGSSI activities, oversees security audits, and provides recommendations.

- The DGSSI issued several guidelines, including the National Cybersecurity Strategy of Morocco. The strategy outlines strategic goals and priorities for addressing digital challenges, and fostering a secure environment for economic and social development. The national cybersecurity strategy includes an action plan extending to 2030 and is subject to periodic review and adjustment by the national authority.

- Additionally, the DGSSI provides manuals for cybersecurity professionals and issues recommendations and best practices for network setup, web applications, and linux, among other documents regulating standards and strategic directions. Finally, the DGSSI regularly issues security bulletins on security breaches and vulnerabilities of information systems.

SOURCES

Primary Legislation

- Law No. 05-20 on Cybersecurity
- Law No. 03-07 complementing the penal code regarding crimes related to automated data processing systems

Secondary Legislation

- General Directorate of Information Systems Security (DGSSI): Decree No. 509-11-2 issued on September 21, 2011 supplementing Decree No. 673-82-2 issued on January 13, 1983 concerning the organisation of the National Defense Department and the establishment of the General Directorate of Information Systems Security
- General Directorate of Information Systems Security (DGSSI): Decree No. 2-21-406 to make Law No. 05-20 of Cybersecurity come into force
- General Directorate of Information Systems Security (DGSSI): Prime Minister's Directive No. 2/2023 issued on January 12, 2023 on the implementation of the National Strategy for Information Systems Security
- General Directorate of Information Systems Security (DGSSI): Prime Minister Directive No. 11-74-3 to create the departments and mandates of the directorates of the General Directorate of Information Systems Security
- Circular of the Head of Government No. 2/2023 of January 12, 2023 for all entities to apply the National Directive on the Security of Information Systems
- Order of the Head of Government No. 3-74-11 14 September 2011 regarding the creation of divisions and services of the directorates under the General Directorate of Information Systems Security (DGSSI)

Guidelines

- General Directorate of Information Systems Security (DGSSI): Presentation of the Cybersecurity Law
- General Directorate of Information Systems Security (DGSSI): National Cybersecurity Strategy
- General Directorate of Information Systems Security (DGSSI): Standards for Qualifying Information Systems Security Operators
- General Directorate of Information Systems Security (DGSSI): National Information Systems Security Directives
- General Directorate of Information Systems Security (DGSSI): Cybersecurity efforts at the National Level
- General Directorate of Information Systems Security (DGSSI): Application Security Assessment Criteria
- General Directorate of Information Systems Security (DGSSI): Cybersecurity Risk Management Manual
- General Directorate of Information Systems Security (DGSSI): Information Systems Security Open Guide
- General Directorate of Information Systems Security (DGSSI): Technical guide related to Linux server security
- General Directorate of Information Systems

SOURCES

Security (DGSSI): Web Application Security Guide
- General Directorate of Information Systems Security (DGSSI): Security Management Manual for Authorisation of Information Systems
- General Directorate of Information Systems Security (DGSSI): Technical guide related to Network Security
- General Directorate of Information Systems Security (DGSSI): Recommendations and best practices for setting up BGP and DNS protocols
- General Directorate of Information Systems Security (DGSSI): Cybersecurity Incident Management Reference
- General Directorate of Information Systems Security (DGSSI): Manual on Industrial Information Systems Security
- General Directorate of Information Systems Security (DGSSI): Guide to Entifying Sensitive Information Systems for Critical Infrastructures
- General Directorate of Information Systems Security (DGSSI): Software Development Lifecycle Security Maturity Assessment
- General Directorate of Information Systems Security (DGSSI): Security Bulletins

Oversight Authorities
- Cybersecurity Strategic Committee
- Serious Cybercrises and Events Management Committee
- General Directorate of Information Systems Security (DGSSI)
- General Directorate of National Security

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. The Digital Development Agency is conducting a project to develop the national AI ecosystem, including support for research and development, as well as skill development. No regulatory agencies have issued guidelines on the application of existing rules to AI.

Summary

- There are currently no public, official sources on primary legislations for AI in Morocco. However, according to news reports, the Moroccan parliament has scheduled a hearing session for September 2024 to explore global best practices and establish a legal framework for AI governance.

  AI features prominently in the Digital Morocco 2030 strategy. The strategy has 2 objectives: stimulating the digital economy and digitising public services. They are achieved through three accelerators (digital talents, cloud, connectivity) as well as "transversal levers," one of which is AI.

- Furthermore, the strategy emphasises that the latest technological innovations are integral, specifically AI. Finally, AI features as part of the "stimulating the digital economy" objective. The positioning of the "national offer on high-value-added sectors such as AI" is a key measure for the vision of upgrading and developing Morocco as an outsourcing and digital export hub.

- In November 2022, the International Center for AI was inaugurated at Mohammed VI Polytechnic University, positioning Morocco as a leader in AI development in Africa. The proposed legislation on AI governance is expected to include provisions for establishing an AI governance agency. This agency would be tasked with overseeing AI development and modernising the national AI strategy.

  AI-related activities fall under the jurisdiction of the Ministry of Digital Transition and Administrative Reform, which is responsible for developing an AI governance framework, and partly the Digital Development Agency (ADD). The Ministry of Digital Transition and Administrative Reform is overseeing the implementation of the UNESCO recommendations on AI Ethics, to which Morocco adhered to in 2022.

- The ADD has published the Morocco AI Ecosystem Guidelines, which aims to establish AI as a catalyst for innovation and economic transformation, to generate new services, jobs, and skills. The approach includes supporting AI research, developing national expertise in Natural Language Processing and Natural Language Generation, and identifying high-potential sectors for AI application.

- In May 2019, the ADD, in collaboration with the National Centre for Scientific and Technical Research (CNRST) and other governmental bodies, launched the Al-Khawarizmi program. This initiative promotes applied research in AI and Big Data, offering a budget of 50 million dirhams to support sectoral AI applications in Morocco.

- Morocco has also participated in the second Global AI Summit that took place in September 2022, under the theme "AI for the Good of Humanity".

  The conference focused on eight key areas: smart cities, capacity building, healthcare, transportation, energy, culture, environment, and economic mobility. During the summit, the member states of the Digital Cooperation Organization adopted the Riyadh AI Call for Action Declaration.

SOURCES

Guidelines

- Digital Morocco 2030
- General Guidelines for Digital Development 2025
- Morocco AI Ecosystem Guidelines
- Presentation of the ADD
- Launch of "AI-Khawarizmi" Programme
- International Frameworks
- General Assembly adopts landmark resolution on AI
- Morocco and the U.S. Launch a “Group of Friends” on AI for Sustainable Development
- UNESCO recommendations on AI Ethics

Oversight Authorities

- Ministry of Digital Transition and Administrative Reform
- Digital Development Agency (ADD)

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 protected works and provides exclusive economic rights to authors. Exceptions include use for the program's intended purpose or by educational institutions, as well as copying for backup or recovery purposes. Morocco does not mandate any form of source code sharing.

Summary

- In Morocco, source code is generally protected under the intellectual property framework described in the Law on Copyright and Related Rights. The law defines a computer program as a series of instructions expressed in words, codes, diagrams or any other form which, once they are incorporated in a carrier that can be deciphered by a machine, are able to accomplish a particular task or obtain a specific result, using a computer or an electronic method able to process the information.

- Computer programs in general are explicitly included in the list of protected works under the copyright law, alongside literary and artistic works, and the economic rights of the author of a computer program include the exclusive right to reproduce, adapt, and distribute the software, among other rights are transferable, subject to the terms of a contract, which usually outlines the specific rights that are transferred or licensed.

- The lawful owner of a copy of a computer program may, without the author's consent and without payment of separate remuneration, make a copy or adaptation of that program provided that such copy or adaptation is necessary for the use of the computer program for the purposes for which the program was obtained or for archiving and backup purposes.

  The reproduction of computer programs is generally not allowed except for under specific conditions, for example when necessary for the use of the program by the authorised user, for backup purposes, or for testing the program's functionality to understand underlying principles.

- The legitimate owner of a copy of a computer program can reproduce or adapt the program without the author's authorisation under certain conditions. These conditions include when such actions are necessary for the use of the program for its intended purpose or for making a backup copy to replace a legally obtained copy that has been lost, destroyed, or rendered unusable.

- Temporary reproduction of a work, including software, is also allowed as long as it takes place during a digital transmission or an act designed to make a digitally stored work perceptible, is carried out by an authorised person or entity, or is of an accessory nature, part of normal use, and is automatically deleted without allowing the recovery of the work for other purposes. Furthermore, the law permits the reproduction of computer programs by educational institutions for teaching or examination purposes, provided that the institution's activities are not commercially oriented and that the reproduction is justified by the aim to be achieved.

- The Moroccan Copyright Office (BMDA) is tasked with ensuring the implementation and enforcement of copyright and related rights in Morocco. It administers and manages the registration of copyrighted works and related rights, including computer programs and software. It maintains records of registered works and manages the distribution of royalties to rights holders, and monitors the use of copyrighted works and takes action against unauthorised use, including initiating legal proceedings against infringers. It collaborates with law enforcement agencies to ensure compliance with copyright laws.

SOURCES

Primary Legislation

- Dahir No. 1-00-20 of February 15, 2000 promulgating Law No. 2-00 on copyright and related rights
- Dahir No. 1-05-192 of February 14, 2006 promulgating Law No. 34-05 amending and supplementing Law No. 2-00 on copyright and related rights
- Dahir No. 1-14-97 of May 20, 2014 promulgating Law No. 79-12 supplementing Law No. 2-00 on copyright and related rights
- Dahir No. 1-22-35 of May 24, 2022 promulgating Law No. 66.19 supplementing Law No. 2-00 on copyright and related rights
- Dahir No. 1-22-52 of August 11, 2022 promulgating Law No. 25.19 on the Moroccan Office of Copyright and Related Rights

- Secondary Legislation
- Decree No. 2.64.406 of March 8, 1965 creating the Moroccan Copyright Office (B.O No. 2732 page 255)

Guidelines

- Presentation of Protected Works by the Moroccan Copyright Office (BMDA)

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 to value-added tax, when delivered to consumers in Morocco. E-commerce imports are subject to both customs duties and value-added tax of up to 20%. As of July 2022, the de minimis value on e-commerce imports of MAD 1250 was abolished. Morocco has not established a direct tax on providers of digital services or digital products and applies standard corporate income tax.

Summary

- Customs duties apply to imports, including e-commerce imports, and are calculated based on the ad valorem value of goods upon entry into Morocco. Duties may be reduced under free trade agreements or specific regulations. Duties apply to all e-commerce imports, since the previous de minimis threshold of MAD 1250 was removed in July 2022. An additional import tax of 0.25% is levied on the value of the imported goods.

- Morocco applies a value-added-tax (VAT) on e-commerce imports and digital services provided by both resident and non-resident entities that are consumed within Morocco. The VAT rate is generally 20%, although a lower 10% rate applies to certain goods, and applies without value thresholds (since the previous de minimis threshold of MAD 1250 was removed). The VAT applies to e-commerce imports and digital services, including the hosting of websites, the provision of digital content, video-on-demand services, and the supply and maintenance of software, among others. Non-resident digital service providers must register for VAT in Morocco and are required to set up systems for collecting and remitting VAT to Moroccan tax authorities.

- For business-to-consumer (B2C) transactions, non-resident providers must register for VAT in Morocco and charge VAT on their supplies to Moroccan consumers. For business-to-business (B2B) transactions, non-resident providers do not charge VAT directly but rather under a reverse charge mechanism.

- The Moroccan Tax Authority and the Ministry of Finance recently issued a circular discussing amendments to the Customs and Excise Code, including to facilitate customs clearance procedures. The circular further describes a significant reform of the VAT system, which will transition to only two base rates by 2026, and clarifies the new VAT system on e-commerce activities. In addition, two decrees specify the application of the VAT.

- The Tax Authority of Morocco has issued multiple guidelines on the Corporate Income Tax (CIT), VAT, and income taxes, covering application scope, taxable transactions, exemptions, and VAT rates.

  Morocco has not established a direct tax on providers of digital services or products and instead applies standard corporate income tax. The 2023 Finance Act sets the corporate income tax rates at 20% for companies with net taxable income below MAD 100 million and 35% for those with net taxable income above MAD 100 million, with certain exceptions.

- In addition, Morocco maintains tax treaties with numerous countries (see list below). The 2024 Finance Act has extended the scope of VAT to dematerialized services supplied remotely by non-residents, even if they have no establishment in Morocco. Foreign service providers thus have to register on a dedicated platform, declare their monthly income and pay the corresponding VAT. This measure includes online training, software and digital content.

SOURCES

Primary Legislation

- General Tax Code 2024
- Finance Law of 2023 [source not available]
- Finance Law of 2024 [souce not working]
- Customs and Indirect Tax Code

Secondary Legislation

- Decree No. 2.06.574 of December 31, 2006 taken for the application of VAT
- Decree No. 2-15-789 of December 21, 2015 taken for the application of Article 179-III of the General Tax Code relating to the recovery of the TSAVA and VAT
- Circular Note No. 717 relating to the General Tax Code - Volume I
- Circular Note No. 717 relating to the General Tax Code - Volume II
- Circular Note No. 717 relating to the General Tax Code - Volume III
- Circular Note No. 6346/210 of July 2022
- Circular Note No. 6522/210 of December 2023 on VAT and Imports

Guidelines

- Tax Authority of Morocco: Summary of the Moroccan Tax System
- Tax Authority of Morocco: VAT Guidelines
- Tax Authority of Morocco: VAT Presentation

International Frameworks

- Morocco Tax Treaties

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.

Morocco generally applies the regulatory framework for the banking, insurance, and payments sector to digital payments, with specific guidelines outlining rules for digital payments. Hence, general know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payments. Similarly, electronic payment providers must obtain non-digital-specific licences by the central bank. Finally, cross-border wire transfers of any value must include specific information about the originator and beneficiary, which must be retained for ten years.

Summary

- The legal foundation for digital payments in Morocco is laid by the Legislative Decree to establish the Central Bank of Morocco (Bank Al-Maghrib or BAM). This decree has been amended several times, most recently in 2019 to further refine the BAM's governance and supervisory roles, enhancing its authority and operational independence. General know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payments.

- Electronic payment providers are required to obtain non-digital-specific licences from the Central Bank of Morocco. This ensures that all payment institutions operate under a consistent regulatory environment, irrespective of whether their services are digital or traditional.

  For cross-border wire transfers, Moroccan regulations mandate that transactions of any value must include detailed information about both the originator and the beneficiary. This information must be retained for ten years to comply with anti-money-laundering requirements and facilitate transparency and traceability in international transactions.

- The Central Bank of Morocco is responsible for overseeing the digital payment systems in Morocco. It issues regulations and circulars to ensure compliance with payment standards and practices.

  The bank's role includes monitoring payment institutions, ensuring adherence to security measures, and managing the approval of new payment technologies.

- The BAM's oversight extends to enforcing technical and operational standards for digital payments, including mobile payments and electronic transactions. Notably, the Competition Council recently ruled to end the card transaction processing monopoly.

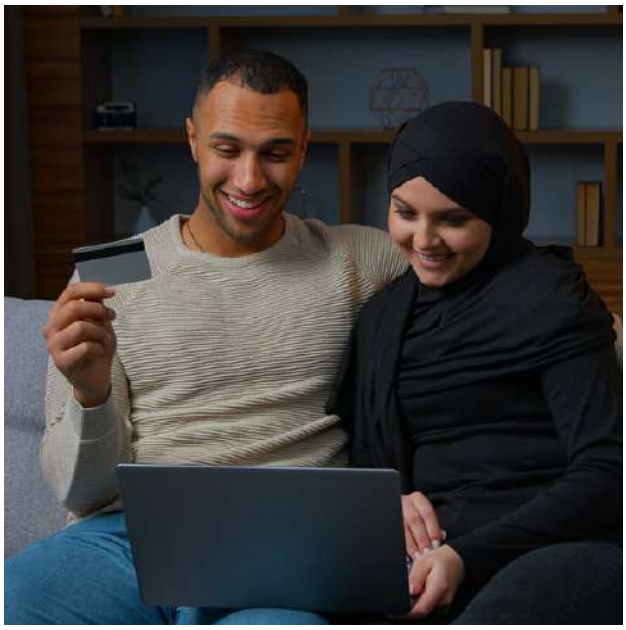
- The regulatory framework includes several circulars and decrees, including on domestic mobile payments and the use of M-Wallets. They specify requirements for authentication, data security, interoperability, and fraud reporting. The Central Bank of Morocco also oversees the technical and security standards for mobile payments systems and the management of M-Wallet services.

- In 2020, the Ministry of Economy and Finance, along with BAM, introduced the National Financial Inclusion Strategy. This strategy aims to enhance mobile payment services, expand financial inclusion, and improve accessibility. Moreover, the

- BAM authorised 16 new payment institutions, reflecting progress in regulatory and technical fields.

- In June 2023, Morocco launched its instant payment system, Virement Instantané, developed by the Groupement pour un Système Interbancaire Marocain de Télécompensation (GSIMT). This system enables transactions between different banks in under 20 seconds and supports amounts up to MAD 20,000. The system aims to include all Moroccan banks, enhancing transaction speed and simplicity across the financial sector.

- The Moroccan Ministry of Economy and Finance, in collaboration with BAM, issued the National Financial Inclusion Strategy, which outlines the development of the mobile payment ecosystem, and include the promotion of interoperability through the SWITCH Mobile platform and efforts to improve the accessibility and availability of mobile payment services, supported by the establishment of technical and functional rules and expansion measures for payment acceptance networks.



- BAM also set up a governance framework to oversee the deployment and sustainability of the mobile payment model and has approved 16 new Payment Institutions authorised to offer payment services.

SOURCES

Primary Legislation

- Legislative Decree No. 233.1.59 to establish the Central Bank of Morocco (Bank Al-Maghrib) [source not working]
- Legislative Decree No. 1.61.258 in the change of the decree regarding the creation of Bank Al-Maghrib [source not working]
- Legislative Decree No. 1.93.386 to amend the Legislative Decree No. 233.1.59 establishing the Central Bank of Morocco [source not working]
- Law 76.03 with regards to the Bylaws of the Central Bank of Morocco [source not working]
- Law No. 40.17 of July 2019 with regard to the Bylaws of the Central Bank of Morocco
- Law No. 43.05 on AML/CFT as amended and completed

Secondary Legislation

- Decree No. 2.80.554 dated October 24, 1980 to change the fourth paragraph in Chapter 35 of Legislative Decree No 233.1.59 issued on June 30, 1959 on the establishment of the Central Bank of Morocco [source not working]
- Regulatory Decision No. 392/W/2018 on domestic mobile payment
- Circular letter No. LC/BKAM/2018/70 on domestic mobile payment
- Systems and Means of Payment Regulatory Framework
- Bank Al-Maghrib Decree N° 392/W/2018
- Bank Al-Maghrib Circular LC/BKAM/2018/70
- Circular no. AS/03/2021
- Circular no. AS/02/2019

Guidelines

- National Financial Inclusion Strategy of Morocco [source not working]
- Cashless payment instruments
- Status of Bank Al-Maghrib
- Collection of regulatory texts adopted pursuant to Law No. 40-17 on the status of Bank Al-Maghrib
- AML and CFT Guideline in Morocco
- Guidelines on Due Diligence
- Institutional brochure
- References to texts involving interactions between BAM and other institutions
- Status and Missions of the BAM
- Competition Council ruling on card transactions

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.

The Moroccan government is currently developing a new strategy for the country's digital transformation and digital economy. Previous such strategies have emphasised the inclusion of SMEs in this process. The Maroc Digital 2020 strategy launched in 2016, for instance, set the goal of connecting 20% of SMEs to the internet.

2

Summary

- Morocco has implemented a range of initiatives to foster digital inclusion for SMEs and disadvantaged groups. These efforts encompass national strategies, dedicated agencies, and targeted programmes aimed at enhancing digital connectivity, facilitating digital transformation, and promoting e-commerce adoption. The initiatives span various sectors and demographics, with a particular focus on women-led businesses, rural enterprises, and recently established companies.

- The Moroccan government's commitment to digital inclusion is evidenced by its national digital strategies. The Digital Morocco 2030 strategy includes exhaustive details for mobilising tech start-ups and powering the digital economy. The Maroc Digital 2020 strategy, launched in 2016, established a target of connecting 20% of SMEs to the internet. To implement these strategies, Morocco established the Digital Development Agency in 2017. This agency oversees programmes such as the Digital SME initiative, which provides financing and comprehensive digitalisation systems to support small businesses' digital transformation. The agency also manages the Smart Factory initiative, which facilitates industrial SMEs' access to Industry 4.0 technologies for digital transformation.

- The National Agency for the Promotion of SME (MarocPME) administers the Mowakaba Digital Transformation programme. This initiative offers financial support to SMEs for acquiring new IT solutions, deploying e-commerce platforms, and promoting overall digital development. Additionally, the Forsa programme, launched in 2022, targets self-employed entrepreneurs and founders of recently established small companies. It provides loans and technical assistance to help these businesses establish a digital presence and digitalise their processes.

- Several initiatives focus on specific segments of the SME economy. The World Bank's WE-FI E-commerce programme, implemented by MarocPME, specifically supports women-led businesses in developing their e-commerce capabilities. This programme offers consulting services from e-commerce advisors, skills training, and preferential rates from partner platforms. In 2023, the World Bank announced development policy financing of USD 450 million to support digital entrepreneurship and access to digital infrastructure and services for Moroccan SMEs.

- Rural and agricultural enterprises are the focus of a project launched in 2022 as part of the MED MSMEs programme. This initiative, a collaboration between the European Union and three Moroccan agencies, aims to encourage digitalisation among small rural and agricultural enterprises. Furthermore, in 2023, the European Bank for Reconstruction and Development and the European Union announced a EUR 20 million loan to the Morocco Bank of Commerce and Industry (BMCI) to support women-led MSMEs, with a strong emphasis on digitalisation.

- The Ministry of Digital Transformation and Public Administration Reform, in collaboration with the German development agency GIZ, has launched a programme to support MSME digital inclusion. This initiative, running from 2023 to 2027, provides technical assistance to facilitate digital adoption among MSMEs.

  The government is emphasising MSME inclusion given their crucial role in the Moroccan economy. The Ministry of Industry and Commerce has set up several initiatives and projects to accelerate the digitisation of the commerce sector, promote electronic payment and encourage the development of e-commerce, including the Moroccan Retail Tech Builder project and e-commerce and digital marketing training courses for retailers.

SOURCES

- Digital Morocco 2030
- Maroc Digital 2020
- Head of Government chairs second meeting of National Commission for Digital Development
- Digital Development Agency: Digital SME
- Digital Development Agency: Smart Factory (model factory 4.0)
- Forsa program
- MarocPME: Mowakaba Digital Transformation
- Maroc PME and World Bank: WE-FI E-Commerce
- World Bank Development Policy Financing (DPF) of $450 million
- EBRD, EU support women-led firms in Morocco, with extended support to earthquake areas
- MES MSMEs: Assessment of the digital maturity and analysis of the digitisation support needs of exporting agribusiness SMEs
- Ministry of Digital Transformation and Public Administration Reform: Digitialsing micro, small and medium-sized enterprises

02
Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Morocco'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 Morocco'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 10.57% of Morocco's imports. The share of advanced technology products in exports was slightly lower at 8.89%, indicating a moderate technology trade imbalance.

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

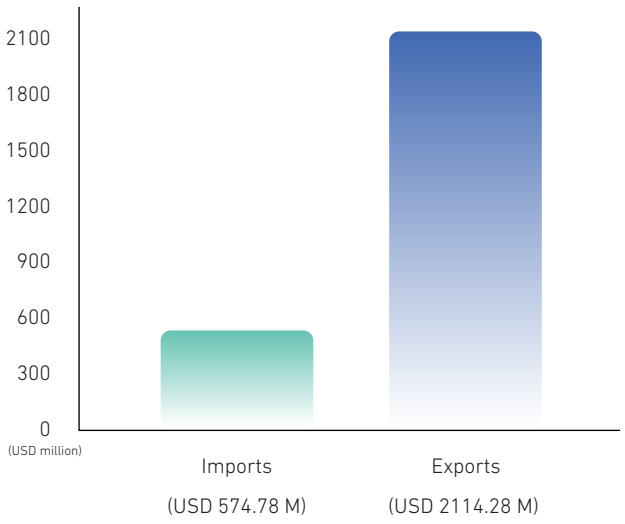


Figure 1 provides data for Morocco's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2: Digital Delivered Services

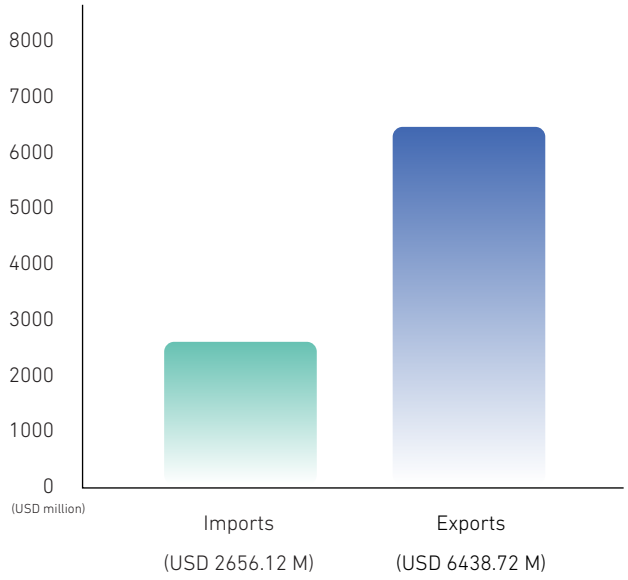


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity (2022)

To analyze Morocco'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

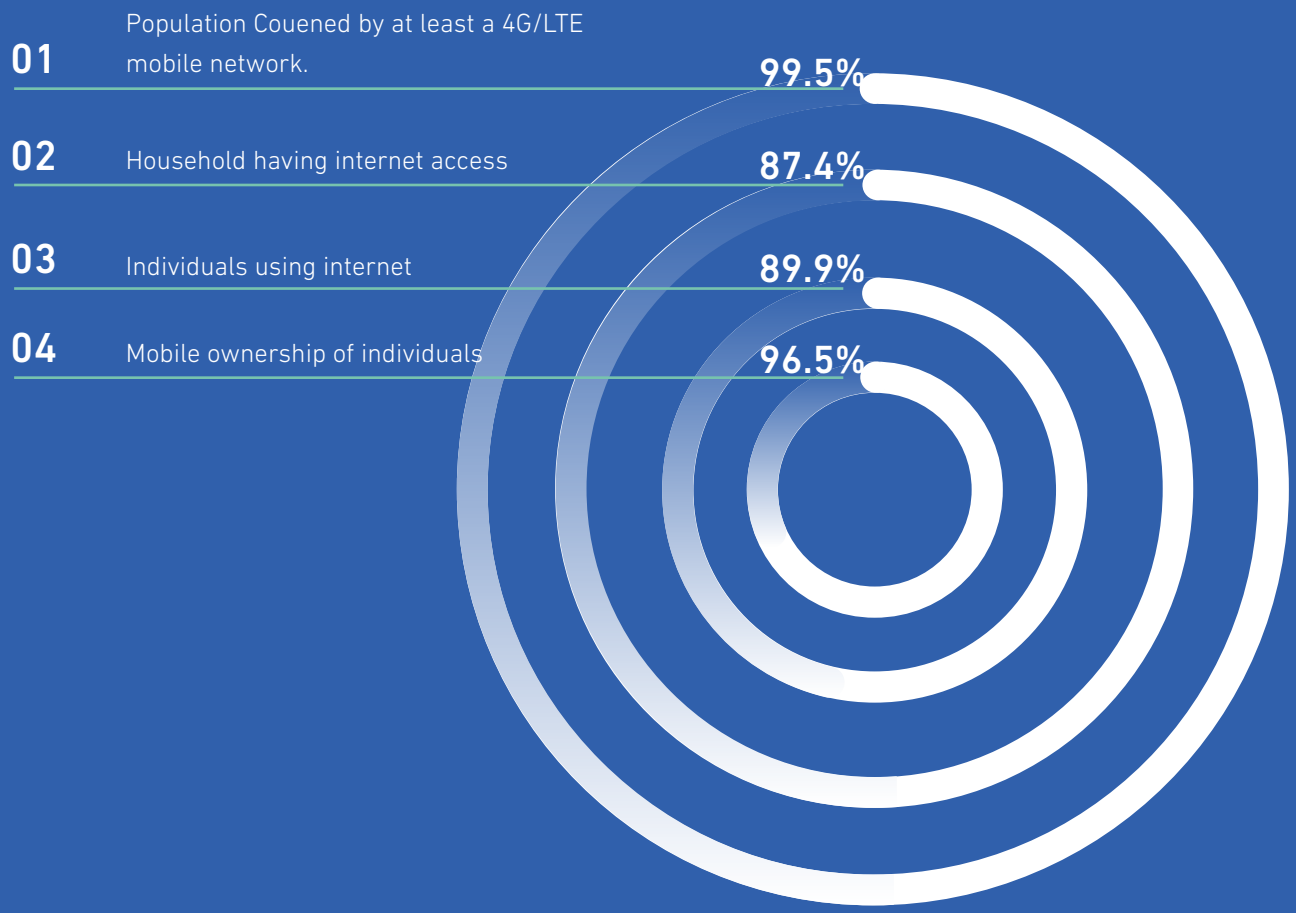


Figure 3 provides data to analyze Morocco's digital infrastructure and connectivity in 2022.

Digital Skills

To document Morocco'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 47.71% in 2023, indicating moderate participation in higher education. The adult literacy rate was 77.35% in 2022. Government expenditure on education as a percentage of GDP was 5.03% in 2023.

The proportion of youth and adults with basic digital skills in Morocco showed varying competency levels:

- 50.39% were able to copy or move a file or folder (2019).
- 20.71% had created electronic presentations with presentation software (2021).
- 40.30% could find, download, install and configure software (2021).

Digital Government

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

In terms of digital government services in 2022, Morocco did not have a government cloud platform. It had a government interoperability framework in draft or planned. It did not have a government open-source software policy or action plan. Morocco maintained both an open government portal and an open data portal.

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

Finally, Morocco 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 either a strategy or program to improve digital skills in the public sector

03 It had either a strategy or program to improve public sector innovation

03 International Commitments and Collaboration

International Commitments and Collaboration

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

Morocco has entered the Morocco - United States Free Trade Agreement which contains provisions pertinent to Electronic Transactions and Customs Duties

Conventions

Morocco 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 Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185) (Cybersecurity)

04 Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) (Cybersecurity)

05 Council of Europe Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (Cybersecurity)

06 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Data Protection)

07 Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) (Data Protection)

08 Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181) (Data Protection)

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

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

11 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, Data Protection)

12 African Continental Free Trade Area Digital Trade Protocol [third-party source] (cross-cutting)

Guidelines, Recommendations, and Principles

Morocco 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 United Nations draft Resolution A/78/L.49 on Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (Artificial Intelligence)

04 Morocco 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 Morocco is a member state of the African Union, that participates in the Group of 20 countries (G20), which has adopted the following frameworks:

11 African Union Agenda 2063
G20/Organisation for Economic Co-operation and Development High-Level Principles on SME Financing (SMEs and Digital Inclusion) (Note: The Principles on SME Financing were adopted in 2015 before the African Union joined the G20 in 2023.)
G20 Artificial Intelligence Principles (G20 Ministerial Statement on Trade and Digital Economy, 2019) (Artificial Intelligence) (Note: The G20 AI Principles were adopted in 2019 before the African Union joined the G20 in 2023.)

Models

Morocco has not adopted or been influenced by any model frameworks.

Other Commitments

01 Morocco 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 Morocco is a member of the African Union, which has adopted the Continental Artificial Intelligence Strategy (Artificial Intelligence) and the Digital Transformation Strategy for Africa (Cross-cutting).

03 Morocco is a member of the African Continental Free Trade Area, which has published the draft Protocol to the Agreement establishing the African Continental Free Trade Area on Digital Trade [Third party source (leak)] (Cross-cutting).

04 Morocco is a member of the Smart Africa Alliance, which has adopted the Artificial Intelligence for Africa Blueprint. (Artificial Intelligence)

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

07 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)

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

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

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

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

Fora

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

01 United Nations Global Digital Compact (Cross-cutting)

02 African Digital Compact (Cross-cutting)

03 European Union - African Union Digital Economy Task Force (Cross-cutting)

04 Arab Federation for Digital Economy (Cross-cutting)

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

06 Smart Africa Alliance (Cross-cutting)

07 African Digital Compact (Cross-cutting)

@dcorg | www.dco.org