8. MOROCCO

Regional Economic Community: Union of Arab Maghreb (UMA)
Population: 36 635 156
Internet Penetration: 23 739 581 users i.e. 64.8% of the population.
AUCC Ratification Status: N/A

8.1. OVERVIEW


ELECTRONIC TRANSACTIONS: Morocco has an electronic transactions law (Law 53/05) and multiple Decrees. The Digital Morocco 2013 strategy considers electronic transactions/e-commerce. The Directorate-General for Information Systems Security (DNSSI) is responsible for approving electronic certification service providers (PSCE's) and the approval of secure electronic certificates.


8.2. DATA PROTECTION

8.2.1. Overview of Data Protection Legislation

At a Constitutional level, Article 24 of the Moroccan Constitution, 2011, expressly guarantees the right to privacy. Thereunder, every person has the right to the protection of his private life. Private communications are considered secret. Encroachments into one's privacy can only be authorised in cases of justice, under conditions set by law (Makulilo, 2016).

Personal data protection is governed in Morocco primarily by Law 09/08 of 18 February 2009 relating to the protection of individuals with respect to the processing of their personal data (“Law 09/08”) and by its implementation, Decree 2-09-165 of 21 May 2009 (“the Decree”). The application of Law 09/08 applies to processing by automatic and non-automatic means whether by juristic/legal and natural persons; whether public or private - Article 2(1).

Law 09/08 has extra-territorial application when the person responsible for the processing uses automated or non-automated means located on Moroccan territory - Article 2(2).

Article 3(1) of Law 09/08 sets out the principles for processing Personal Data and requires that Personal Data must be:

- processed fairly and lawfully;
- collected for explicit and a legitimate aim only;
- not further processed in a way incompatible with the stated purposes;
- adequate, relevant and not excessive in relation to purposes for which they were collected and for which they are further processed;
- accurate and up to date and where inaccurate, incomplete or outdated, all reasonable measures must be taken to ensure that such Personal Data are erased or rectified; and
- kept in a form which permits identification of data subjects for no longer than that which is necessary to achieve the purposes for which they were collected and for which they are further processed.

The processing of Sensitive Data must be in adherence with the processing conditions set out under Law 09/08, failing which prior authorisation must be provided by the National Control Commission for the Protection of Personal Data (CNDP).

Article 4 sets out the requirements for valid consent as a condition for lawful data collection and Articles 5 - 9 set out and grant data subjects with the following rights:

- Information regarding the use of data (Articles 5-6);
- A right to access to data held, as well as their origins and destinations (Article 7);
- A right to rectification, without charge (Article 8);
- A right of appeal to the CNDP; and
- A right to express opposition to the collection of the data (Article 9).
Instances where prior authorisation is required from the CNDP before processing may commence/continue are detailed under Article 12 of Law 09/08 as well as Article 21 (for sensitive data). In terms of Article 22, the processing of health data is subject to a declaration to the CNDP.

Section 3 (Articles 23-36) set out the confidentiality, security and storage obligations of controllers and subcontractors (as defined under Law 09/08).

**Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”)**

Morocco ratified Convention 108 on 28 May 2019. In addition to providing guarantees concerning the collection and processing of personal data, in the absence of proper legal safeguards, Convention 108 prohibits the processing of “sensitive data” which includes data relating to a person’s race, political views, health, religion, sexual life, and criminal record. The Convention also provides individuals with a right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

On 6 June 2013, Morocco adopted a Bill approving Convention 108 (Makulou, 2016, 37), thereby acceding to Convention 108.

**Francophone Binding Corporate Rules**

The Kingdom of Morocco is also a member of the French Speaking Association of Data Protection Authorities (Association francophone des autorités de protection des Données personnelles – “AFAPDP”). The Francophone Binding Corporate Rules on transfers of personal data (Les Règles Contraignantes d’Entreprise Francophones (RCEF)) were adopted by Morocco in 2013 and Morocco is bound thereby.

**8.2.2. Data Protection Policy Developments**

The Digital Morocco 2013 strategy is the core policy document containing policy actions for data protection. Thereunder, Morocco has, amongst other things, strategized to:

- Implement a law relating to data protection (Action 3.1 of Initiative 3) – achieved; and

- Allocate a budget to establish the National Commission for Data Protection (CNDP) (Budget 48) – achieved.

**8.2.3. Data Protection Institutional Measures**

The following institutions are relevant to Data Protection in Morocco:

- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (“CNDP”) (which translates to the ‘National Control Commission for the Protection of Personal Data’): The CNDP is the independent administrative authority in charge of protecting personal data in Morocco, established by way of Decree 2-11-508. The CNDP is an autonomous authority charged with ensuring that the use of personal data does not prejudice personal privacy. The CNDP has authority over private and public institutions and their conformity with Law 09/08. The CNDP also has the power to take judicial action and apply financial and penal sanctions, in the event of infringements of the Law 09/08.
  - In January 2014, the CNDP launched its first large-scale control operation to verify the compliance by Moroccan websites and online businesses with the provisions of Law 09/08. Contravening websites were invited to comply with the law. Past a certain deadline, CNDP warned that non-compliant online businesses could face sanctions, including legal action (CNDP, 2014).
8.3. Cybercrime and Cybersecurity

8.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Morocco are primarily governed by the following laws/legislative instruments:

- Law No. 07/03 supplementing the Penal Code with respect to offenses relating to automated data processing systems (“Law 07/03”);
- Decree 2-15-712: On the protection of sensitive information systems and critical infrastructures; and
- Decree 2-11-509: Completes Decree 2-82-673 on the organisation of the national defence administration with provisions on cybersecurity and information systems security.

**Law 07/03**

Since November 2003, cybercrime has been deemed a criminal offence in Morocco. Through Law 07/03, the Moroccan Criminal Code was updated to include and define cybercrime as “offenses related to automated data processing systems” Specifically, the crimes supplemented include:

- Fraudulently modifying/altering all or any part of an automated system (Article 607-3);
- Fraudulently modifying/altering all or any part of an automated system for the purposes of obtaining information relating to the internal or external secrets of the State or the national economy (Article 607-4);
- The intentional hindering or distorting of an automated data processing system (Article 607-5);
- The fraudulent introduction of data in an automated data processing system that deteriorates, removes or modifies the data it contains, their method of processing or transmission (Article 607-6); and
- Forgery or falsification of computerized documents, regardless of form, that is likely to cause prejudice to others (Article 607-7).

Apart from the foregoing, the extent to which Morocco has adapted traditional offences to ICTs (for example, those pertaining to intellectual property), is unclear.

**Decree 2-15-712**

Decree 2-15-712 on the Protection of Sensitive Information Systems and Infrastructures of Vital Importance regulates the protection of Morocco's critical information systems and infrastructure.

**Decree 2-11-509**

Decree 2-11-509, as read with Decree 2-82-673, confers statutory authority and legal capacity on a national regulatory authority (the Directorate-General for Information Systems Security – “DGSSI”) which is responsible for all aspects of Morocco’s national cyber security.

8.3.2. Cybercrime and Cybersecurity Policy Developments

In 2012, CSSSI adopted Morocco’s first National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) built on the National Strategy for Information Society and Digital Economy ("Digital Morocco 2013 strategy") and focused on four main strategic priorities, namely:

- evaluating risks to information systems within government and in vital infrastructures;
- protecting the information systems of government agencies, public organizations, and vital infrastructures;
- strengthening the foundations of information systems security (legal framework, sensitization, training, research and development); and
- promoting national and international cooperation.

CSSSI also developed an action plan for DGSSI “to operationalize the guidelines and directives included in the strategy.”

*Figure 4: Morocco Cyber Readiness (Source: Kingdom of Morocco Cyber Readiness At A Glance - Melissa Hathaway and Francesca Spidalier)*

Under the Digital Morocco 2013 strategy, the promotion of cyber-confidence is recorded as a priority. The Digital Morocco 2013 strategy also acknowledges the nexus between the security of information systems and the successful uptake and expansion of Morocco’s e-commerce industry.

In 2013 Morocco also introduced the National Security Directive on Information Systems, which, amongst other things, sets out an action plan for the protection of ‘infrastructure of vital important’ (critical infrastructure). One of the core actions of this Directive is to develop and implement a National Directive of Information Systems Security (DNSSI).
8.3.3. Cybercrime and Cybersecurity Institutional Measures

In accordance with its National Cybersecurity Strategy (2013), Morocco has established the following cyber security and cybercrime related institutions in order to “strengthen national capacities as regards the security of the information systems of the administrations, public bodies and infrastructure of vital importance” (Royaume Du Maroc Administration de la Défense Nationale, 2012, 8):

- The Strategic Committee for the Security of Information Systems (CSSSI);
- The DGSSI (as described above);
- The DNSSI: The primary objective of the DNSSI is to raise the level of protection and the level of maturity of the security of all information systems in the Kingdom of Morocco; and
- The Moroccan Computer Emergency Response Team (”ma-CERT”): In 2013 the ma-CERT was established, and it joined the international Forum of Incident Response and Security Teams (FIRST).

In a media statement, the head of the data protection authority CNDP, Saïd Ihrai, stated that Morocco had put in place 29 units specialized in the fight against cybercrime (CIO Mag, 2018). In February 2016, the Moroccan Ministry of Industry launched the “National Campaign to Fight Cybercrime” - an initiative particularly aimed at supporting the private sector. In July 2016, the Ministry of Justice, together with the Council of Europe, organized an international workshop in the capital Rabat, on best practices regarding cybercrime legislation and electronic evidence.

8.4. ELECTRONIC TRANSACTIONS

8.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Morocco are primarily governed by:

- Law 53/05 relating to the electronic exchange of legal data (“Law 53/05”);
- Decree 3-88-13 of January 20, 2015 fixing the form and content of the application for prior authorization for import, export, provision, exploitation or use of means or services of cryptography and the accompanying file;
- Decree 3-89-13 of January 20, 2015 setting the model of specifications to accompany the application to be made by the persons not having the accreditation of certification service providers and who intend to provide cryptographic services subject to authorization; and
- Decree 3-90-13 of January 20th, 2015 fixing the model of specifications to accompany the application for approval of electronic certification services.

Law 53/05

Law 53/05 is the foundation for Morocco’s electronic landscape in that it sets out a regime applicable to legal data exchanged electronically, electronic evidence, cryptography and electronic certifications.

Under Article 3 of Law 53/05, electronic mechanisms may be utilised to make public contractual offers and conclude free exercise of electronic commerce activities.

Article 3-4 as read with Articles 26-27 set out obligations on suppliers to provide consumers with information about the characteristics of goods or services and the details of the supplier in order to enable consumers to enforce their rights and opt-out of communications.

Articles 4 - 5 of Law 53/05 maintains that electronic writing has the same probative value as manuscript writing, provided that the person from whom it emanates can be duly identified and that it is established and preserved in conditions to guarantee the ‘integrity’ thereof.

Article 6 provides for the creation and retention of electronic signatures that ensure the validity thereof through certification by accredited electronic certification providers; and

Articles 12 – 14 set out the basis for the usage of cryptography by accredited electronic certification providers to guarantee the security of the exchange and / or the storage of legal data by electronic means.

Section III of Article 3 of Law 53/05 sets out the basis for the validity of electronic contracts, specifying what constitutes a valid electronic offer and acceptance.

Articles 15-16 of Chapter II of Law 53/05 establishes and regulates the National Authority for approval and supervision of electronic certification, whilst Section II of Chapter II regulates electronic certification service providers.
Information Disclosures, Contractual Liability of Service Providers and Advertising by Electronic Means are also provided for under Law 53/05. Specifically, a framework for information disclosures and terms and conditions by e-commerce providers, as well as contractual liability of such providers, is provided for in Article 3 of Law 53/05. Insofar as advertising by electronic means is concerned, the primary source of regulation is not Law 53/05 but rather Law 09/08 and Morocco’s proposed Bill No. 31/08 on consumer protection, including some provisions concerning the remote sales, online advertising and spamming (“Bill 31/08”). That said, within Article 10 of Law 09/08, an e-commerce provider may not direct market to a data subject, via any electronic means (email, fax, SMS, automated calling machines), unless the recipient has affirmatively consented (as defined in Law 09/08) to such prospecting. Article 10 does, however, make an exception for prospecting to a data subject via e-mail when such information was directly collected from a data subject. In addition, under Bill 31/08, rights for consumers (including e-commerce consumers) are sought to be strengthened.

Articles 38 - 50 of Chapter 4 regulates the advertisement of promotional offers, whilst Article 55-59 of Bill 31/08 deals with advertising of lotteries.

Lastly, sanctions for non-conformity with Law 53/05 are contained within Chapter III. These sanctions contain both monetary penalties, as well as imprisonment.

8.4.2. Electronic Transactions Policy Developments

The primary strategy concerning electronic commerce in Morocco is the Digital Morocco 2013 strategy. The strategy recognised that the adoption of, and interaction with e-commerce is still under-developed for both individuals and enterprises in the Kingdom. The strategy furthermore acknowledged that in order for an uptake in e-commerce (by online sellers and consumers) to take place:

- consumer trust will need to be strengthened through legislative interventions – primarily protecting their personal data, and regulating the relationship between online sellers, and the consumer (Initiative 1 of the Digital Morocco Strategy, 2013); and
- support mechanisms to assist social operators on issues related to Information Systems Security should be implemented.

8.4.3. Electronic Transactions Institutional Measures

The following institutions play a fundamental role in Morocco’s e-commerce:

- The DGSSI: their role insofar as electronic commerce is concerned includes approving electronic certification service providers (PSCE’s) and the approval of secure electronic certificates issued by PSCE’s; and
- The CNDP: the role of the CNDP insofar as electronic commerce is concerned, primarily relates to consumer protection (especially in online environments). Where electronic marketing is concerned, In January 2016, the CNDP issued recommendations regarding unsolicited electronic marketing. It called for the creation of a national opt-out list in which consumers would register to stop receiving commercial marketing messages. This raised the question of a potential misuse of databases that could be exploited for uses beyond the original intended purpose/s. The CNDP recommended establishing a permanent working group to ensure the proper implementation of its recommendations (CNDP, 2016).
8.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

<table>
<thead>
<tr>
<th>Policy and Governance Measures</th>
<th>Legislative and Regulatory Measures</th>
<th>Institutional Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Policy</strong> which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures&lt;br&gt;Morocco has a National Security Directive on ‘Information Systems’ dealing with Critical Infrastructure.</td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;Personal data protection is governed by Law 09/08 of 18 February 2009 and by its implementation, Decree 2-09-165 of 21 May 2009.&lt;br&gt;<strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;Primarily governed by Law 53/05; And&lt;br&gt;Decree 2-82-673 of 28 Rabi I 1403 (13 January 1983); Decree 3-88-13 of January 20; Decree 3-89-13 of January 20, 2015; and Decree 3-90-13 of January 20th, 2015.</td>
<td><strong>Data Protection Authority</strong> whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data&lt;br&gt;The Decree 2-11-508 establishes the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (“CNDP”) (which translates to the ‘National Control Commission for the Protection of Personal Data’) as the authority.&lt;br&gt;<strong>Electronic Signature Accreditation Authority</strong> that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications&lt;br&gt;The Directorate-General for Information Systems Security (“DGSSI”) is the authority.&lt;br&gt;<strong>State Department to regulate and approve electronic commerce payment methods</strong>, only approved payment methods may be validly used in the Member State territory;&lt;br&gt;<strong>State Department to regulate vulnerability and safety guarantee assessments of ICT product vendors</strong> including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers&lt;br&gt;Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).&lt;br&gt;Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation&lt;br&gt;The Strategic Committee for the Security of Information Systems (CSSSI);&lt;br&gt;The Directorate-General for Information Systems Security (“DGSSI”); And&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).&lt;br&gt;Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong>&lt;br&gt;Morocco adopted a National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information).&lt;br&gt;<strong>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</strong>&lt;br&gt;The Ministry of Industry launched the “National Campaign to Fight Cybercrime” - aimed at supporting the private sector.</td>
<td><strong>Cybercrime Laws and Regulations</strong>&lt;br&gt;Cyber security and crimes are primarily governed by Law No. 07/03; And&lt;br&gt;Decree 2-15-712; Decree 2-11-509; and Decree 2-82-673.</td>
<td><strong>Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution</strong>&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).&lt;br&gt;Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation&lt;br&gt;The Strategic Committee for the Security of Information Systems (CSSSI);&lt;br&gt;The Directorate-General for Information Systems Security (“DGSSI”); And&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).&lt;br&gt;Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)&lt;br&gt;The Moroccan Computer Emergency Response Team (“ma-CERT”).</td>
</tr>
</tbody>
</table>

---

MOROCCO
Disclaimer

This report was prepared independently by EndCode.

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AUDA-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AUDA-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AUDA-NEPAD.

About EndCode

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.