FACTSHEET: MOROCCO

Last updated: 30 September 2019
Prepared by Justin Bryant

FAST FACTS

Population: 35,740,000
Capital: Rabat
Prime Minister: Saadeddine Othmani
2019 Freedom House Score: 39/100
Data protection law? Enforced

LAW

In 2009, Morocco enacted Law No. 09-08 relating to protection of individuals with regard to the processing of personal data and its corresponding implementation decree, Decree No. 2-09-165 (referred to collectively as DP Law). The legislation—which created an independent data regulator in the *Commission Nationale de Protection des Données Personnelles* (CNDP)—was progressive for its time.

While Morocco's data protection framework is still well-ahead of many jurisdictions in Africa, it lags behind leading international standards. In a 2018 meeting with an EU delegation, the shortcomings were highlighted—including a lack of detailed conditions related to the validity of consent, the lack of requirements to notify the authority of data breaches, the absence of a data minimization principle, and limits of powers granted to the CNDP.

Under the DP Law, data subjects have the right to:

- have their personal data corrected;
- access their personal data and the reasons for its processing;
- object to the further processing of their personal data, at any time;
- prevent processing of personal data for purposes of direct marketing; and
- object to a decision based solely on automatic processing that would significantly affect the or produce adverse legal repercussions for them.

PERSONAL DATA

Personal data is any information regardless of its nature and format, relating to an identified or identifiable person.

Sensitive data is personal data that reveals the **racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership of the person concerned, or information relating to his, her or their health, including genetic data**.

Sensitive data shall not be processed without affirmative consent from the data subject or unless an exception applies.

COLLECTION AND PROCESSING

Personal data must be:

- processed fairly and lawfully;
- processed to the extent necessary, relevant, and not to excess;
- collected for specific, explicit and legitimate purposes;
- accurate and kept current; and
- kept in a form enabling the person concerned to be identified.

Prior consent from the data subject is generally required for processing, but consent is unnecessary when the information concerns:

- compliance with a legal obligation;
- the commencement or execution of a contract to which the data subject is a party;
- the protection of the vital interests of the data subject, if he or she cannot consent;
- the performance of a task of public interest or related to the exercise of public authority; or
- the fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the data subject.

REGISTRATION AND ENFORCEMENT

As the data protection authority, the CNDP can:

- receive and respond to complaints of individuals' personal data being put at risk;
- appraise elements of litigation arising out data protection law on behalf of courts;
- assist the government in preparing and defining Morocco's position on personal data protection in international negotiations; and
- cooperate with analogous bodies in foreign states.

The CNDP also is granted certain powers, including:

- investigative powers allowing its agents, to collect and seize all information and documents necessary to fulfill its functions and examine facts surrounding complaints;
- the power to levy sanctions on data controllers that violate the DP Law;
- the power to make amendments to the law necessary for safekeeping of data; and
- the power to order the locking, erasure or destruction of data, and to temporarily or definitively prohibit the processing of personal data anywhere on the national territory.

CROSS-BORDER TRANSFER

Personal data is transfers outside Morocco require prior authorisation from the CNDP.

The person in charge of the processing operation can only transfer personal data to a foreign state if the state has an adequate level of privacy protection regarding the data, unless:

- The data subject has expressly consented to the transfer; or
- The transfer and subsequent processing are required for:
    - compliance with a legal obligation;
    - the commencement or execution of a contract to which the data subject is a party;

- the protection of the vital interests of the data subject, if he or she cannot consent;
- the performance of a task of public interest or related to the exercise of public authority; or
- the fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the data subject.

SECURITY AND BREACH PROTOCOL

The DP Law has no specified breach protocol, but it requires data controllers to implement appropriate technical measures and organisational structures to protect personal data breaches or other unlawful treatment. These measures must be appropriate given the level of security risk presented by the processing and the nature of the data in question.

Read the legal notice and terms of use for this factsheet.