DATA PROTECTION LAWS OF THE WORLD

Morocco

DLA PIPER

MOROCCO

Last modified 28 January 2015

LAW IN MOROCCO

Personal data protection is governed in Morocco by the Law n° 09-08 of 18 February 2009 relating to the protection of individuals with respect to the processing of personal data (the 'Law') and by its implementation Decree n° 2-09-165 of 21 May 2009 ('Decree').

DEFINITIONS

Definition of personal data

Personal data is defined by article 1.1 of the Law as any information of any nature and independently of its format, including the sound and images relating to an identified or identifiable individual, referred to in the Law as a 'concerned individual.' A person is deemed identifiable when he or she can be identified directly or indirectly, especially by reference to an identification number or one or several specific elements of his or her physical, physiological, genetic, psychological, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive data is defined by article 1.3 of the Law as 'any information pertaining to a 'concerned individual' that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern sex life or health, including the genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP') (in English 'National Control Commission for the Protection of Personal Data')

6 *Boulevard Annakhil immeuble Les Patios*
3ème ètage
Hay Riad – Rabat, 10000 Morocco

T +212 537 57 11 24
F +212 537 57 21 41

contact@cndp.ma

REGISTRATION

The processing of personal data requires a prior notification to the CNDP.

The processing of sensitive data or of personal data that includes ID card numbers requires a prior authorisation from the CNDP.

The prior notification or authorisation application to the CNDP must specify, among other things:

- the purpose(s) of the processing
- the identity and the address of the data controller (ie the natural or legal person who determines the purpose and the means of the processing of the personal data and either implements such decisions itself or engages a data processor to implement them)
- the possible connections between databases
- the personal data processed and the categories of persons about whom personal data are processed
- the time period for which the data will be retained
- the department or person(s) in charge of implementing the data processing
- the recipients or categories of recipients of the personal data, and
- the measures taken to ensure the security of the processing. Additional specific security measures are required when processing sensitive data.

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Any personal data must be processed consistently with the following general principles:

- all personal data must be processed fairly and lawfully
- all personal data must be collected for specific, explicit and legitimate purposes and be subsequently processed in accordance with these purposes for which they are collected, and
- all personal data must be accurate, comprehensive and, when necessary, kept up to date.

The processing of personal data shall have received the individual's consent or shall fulfill one of the following conditions:

- processing is required by law
- the purpose of the processing is to save the individual's life
- the purpose of the processing is to carry out a public service
- the processing relates to the performance of a contract to which the concerned individual is a party, or
- the processing relates to achieving a legitimate interest of the data controller, balanced against the interests and fundamental rights and liberties of the concerned individual.

Where sensitive personal data are processed, a different list of specific conditions applies. Indeed, the concerned

individual must give his/her express consent for this processing unless the processing meets one of the following conditions:

- the processing is necessary for the exercise of legal or statutory functions of the controller
- the processing is necessary to protect the vital interests of the concerned individual, and that the concerned individual is in physically or legally incapable to give his/her consent
- the processing relates to data made public by the concerned individual, or
- the processing regards the recognition, exercise or defense of legal claims and is done exclusively for this purpose.

The person from whom the personal data is collected must receive notice of:

- the identity of the data controller and, if applicable, the data processor
- the purposes of the data processing; the recipients or categories of recipients of the data, and
- the right to object, for a legitimate reason, to the collection of such data, the right to access the collected data and the right to have the processed data rectified.

TRANSFER

The transfer of a data subject's personal data to another country is allowed if the country provides a sufficient level of protection in relation to an individuals' private life and fundamental rights and liberties. The sufficient nature of the protection is evaluated with regards to national laws and applicable security measures.

Data controllers may transfer personal data out of Morocco to countries that are not deemed to offer adequate protection if the transfer is necessary:

- to safeguarding the individual's life
- to safeguarding the public interest
- to comply with obligations relating to the recognition, exercise or defence of a legal right
- to the consultation of a public register intended to inform the public
- to the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request, and
- to the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

SECURITY

The entity processing the data must take all reasonable precautions with regard to the nature of the data and the risk presented by the processing, in order to preserve the security of the data and, among other things, to prevent third parties gaining unauthorised access to such data. Where sensitive data are processed, the law sets forth specific security requirements that must be followed.

A data processor may only process personal data based upon the instructions of the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality. However, the data controller remains liable for

the processor's compliance with these obligations.

BREACH NOTIFICATION

The Law does not set out any obligation to notify the CNDP or the concerned individual in the event of a data security breach.

ENFORCEMENT

The CNDP is responsible for enforcing the Law.

Violations of the obligations set forth in the Law are punishable as an administrative and/or criminal offence.

Article 50 to 64 of the Law makes it a violation for any person intentionally to:

- fail to notify or seek CNDP's authorisation for data processing
- provide false information in the notification or in the applications for authorisation for the processing of personal data
- misappropriate or uses personal data in a manner incompatible with the purpose of the collection
- promote or carry an illegal collection of personal data, or
- fail to comply with the obligations set forth in the Law or the Decree.

The above offences are punishable by a fine ranging from MAD 10,000 (approx. US$1,200) to MAD 600,000 (approx. US$72,000) and/or imprisonment from three months to four years.

In addition, where the offender is a legal entity, it may be subject to the following penalties:

- partial seizure of its material goods
- seizure of objects and things whose production, use, carrying, holding or selling is an offence, and
- closure of the entity's premises where the offence was committed.

ELECTRONIC MARKETING

Article 10 of the Law provides that advertising/promotion via any electronic means (eg email, fax, SMS) is forbidden if the recipient has not affirmatively consented to it. However advertising and promotion are allowed when the data were collected directly from the recipient.

Unsolicited emails can only be sent without consent if:

- the contact details were provided in the course of a sale
- the marketing relates to a similar product, and
- the recipient was given a method to opt-out of the use of their contact details for marketing when they were collected.

In addition, the Law also prohibits the use of automated calling systems without the consent of the recipient.

Direct marketing emails may not disguise or conceal the identity of the sender. SMS marketing is also likely to be included within this prohibition on email marketing.

The restrictions on marketing by email only apply to email marketing sent to individuals and not to email marketing sent to corporations.

ONLINE PRIVACY

The Law does not specifically address the collection of location and traffic data by public electronic communications services providers, or the use of cookies (or similar technologies).

KEY CONTACTS

Hajji & Associés
www.ahlo.ma

Amin Hajji
Partner
T +212 522 48 74 74
a.hajji@ahlo.ma

Moulay El Amine EL HAMMOUMI IDRISSI
Senior Lawyer
T +212 522 48 74 74
moulay@ahlo.ma

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.