DATA PROTECTION LAWS OF THE WORLD

Algeria

ALGERIA

Last modified 22 December 2022

LAW

Law No. 18-07 of 10 June 2018 on protection of natural persons in personal data processing (“**Law No. 18-07**”).

DEFINITIONS

Definition of Personal Data

Any information, regardless of the medium, relating to an identified or identifiable person, hereinafter referred to as "data subject", directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, biometric, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the data subject or relating to health, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

An independent administrative authority for the protection of personal data, known as the "national authority", is hereby established, with its headquarters in Algiers.

The national authority is responsible for ensuring that the processing of personal data is carried out in accordance with the provisions of the law and for ensuring that the use of information and communication technologies does not pose a threat to the rights of individuals, public freedoms and privacy.

However, although Law No. 18-07 provides for the existence of a national authority, it has not yet been set up.

Presidential Decree No. 22-187 dated 18 May 2022 appointed the President and members of the National Authority for Personal Data Protection.

As said above, the national authority has not yet been made accessible to the public. However, it may soon become operational.

REGISTRATION

Any processing of personal data is subject to prior declaration to or authorisation by the national authority.

The prior declaration, which includes an undertaking that the processing will be carried out in accordance with Law No. 18-07, is filed with the national authority. It may be made by electronic means.

However, as the national authority has not yet been set up, this procedure is not yet applicable.

DATA PROTECTION OFFICERS

The data controller shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

COLLECTION & PROCESSING

Personal data processing may only be processed with the express consent of the data subject. The data subject may withdraw his / her consent at any time.

However, in some cases, consent is not required if the processing is necessary.

The person concerned by the collection of their data has a right to information, a right of access, a right of rectification and a right to object to their data being collected.

TRANSFER

The data controller may only transfer personal data to a foreign State with the authorisation of the national authority in accordance with Law No. 18-07 and if that State ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing of such data.

In any case, it is forbidden to communicate or transfer personal data to a foreign country, when such transfer is likely to affect public security or the vital interests of the State.

However, as the national authority has not yet been established, the consent of the data subject is required.

SECURITY

The controller must put in place measures to ensure the integrity and protection of the data.

These measures must ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

If the processing is carried out on behalf of the controller, the controller must choose a processor providing sufficient guarantees in respect of the technical and organisational security measures relating to the processing to be carried out and must ensure compliance with those measures.

Transfer of data abroad

The foreign State must ensure an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to data processing.

The adequacy of the level of protection provided by a State is assessed in particular by the security measures applicable there.

BREACH NOTIFICATION

Administrative measures

In case of violations of the provisions of Law No. 18-07 by the controller, administrative measures are taken by the national authority:

- warning;
- formal notice;
- provisional withdrawal for a period not exceeding one year, or definitive withdrawal of the declaration receipt or authorisation;

- a fine.

The national authority may also impose fines on the controller which:

- refuses, without legitimate reason, the rights of information, access, rectification or opposition;
- fails to make the required notifications to the national authority.

Criminal sanctions

Violation of the provisions of Law No. 18-07 is punishable by imprisonment and / or a fine.

Companies that are processing personal data at the time of the enactment of Law No. 18-07 must comply with its provisions within a maximum of one (1) year from the date of installation of the national authority.

Mandatory breach notification

Where the processing of personal data over electronic communication networks results in the destruction, loss, alteration, disclosure or unauthorised access of such data, the service provider must notify the national authority and the data subject without delay where such a breach may affect the privacy of the data subject.

Failure by a service provider to notify the national authority or the data subject of a personal data breach is punishable by imprisonment and a fine.

ENFORCEMENT

The application of the sanctions listed under the above headings is relatively limited, as the national authority is not yet established.

However, offences committed by the data controller may be subject to criminal prosecution (without the need for action by the national authority).

ELECTRONIC MARKETING

Law No. 18-05 of 10 May 2018 on electronic commerce provides that the e-provider who collects personal data and builds up customer and prospect files must only collect the data necessary to conclude commercial transactions. It must:

- collect the consent of e-consumers prior to the collection of data;
- guarantee the security of information systems and the confidentiality of data;
- comply with the relevant legislative and regulatory provisions.

ONLINE PRIVACY

Not applicable.

KEY CONTACTS

L& P Partners

Benaouda Miloudi
Associate
T +213 (7) 93 99 92 34
bmiloudi@dz-lpp.com

DATA PRIVACY TOOL

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