FACTSHEET: TUNISIA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 11,782,219
Capital: Tunis
President: Kais Saied
2020 Freedom House Score: 70/100
Data protection law? Enforced

LAW

Tunisia updated its 1959 Constitution to include the right to personal data protection in 2002. Two years later, the Ministry of Justice outlined this right in the Organic Act No. 2004-63, which established the Tunisian data protection authority, the *Instance nationale de protection des données à caractère personnel* (INPDP). At that time, it made Tunisia one of the most progressive regimes for personal data protection in the world.

However, under the authoritarian rule of Ben Ali, few, if any of these rights, were actually realised by the people. Although the Tunisian Jasmine Revolution of 2011 brought democratic reforms, it wasn't until 2015 that data processors began to regularly declare their personal data processing to the INPDP, which, up until that time, had neither been functioning as an independent body, nor was it sanctioning violators of the Organic Act.

Although Tunisia enacted a new constitution in 2014, the old data protection regime remains. During a 2018 conference, Chawki Gaddes, the president of the INPDP, emphasised the importance of modernising the law toward greater effectiveness, and to reflect new social and technological realities as well as Tunisia's new political environment that values democracy and human rights. Given that Tunisia has signed the Council of Europe's Convention 108, the updated Tunisian data protection law will likely reflect the principles therein.

Under Organic Act No. 2004-63, data subjects, their heirs, or their guardians have the right to:

- access all personal data concerning them;
- correct, complete, rectify, update, modify, clarify, or delete when the data is inaccurate, equivocal, or when its processing is prohibited;
- object, at any time, to the processing of personal data concerning them for valid, legitimate and serious reasons, except where the treatment is planned by law or is required by the nature of the obligation; and
- prevent personal data from being shared with third parties for advertising purposes.

However, it is important to note that organisations with a "public personality" (such as police stations, tribunals, and universities) are not bound by the obligations that generally apply to personal data processors in Tunisia. Public organisations are not required to declare data processing and therefore the rights of individuals to their data are limited in their interactions with these entities.

PERSONAL DATA

Personal data is all information regardless of its origin or form, which directly or indirectly allows for the identification of a natural person, with the exception of information related to public life or considered as such by law.

The processing of personal data related to the following categories is prohibited:

- racial or genetic origins;
- religious beliefs;
- political opinions;
- philosophical or union activism;
- health and scientific research; and
- criminal history and proceedings, criminal prosecution, penalties, preventative measures, or judicial history.

COLLECTION AND PROCESSING

The following principles generally apply to the processing of personal data:

- Personal data must be collected directly from the data subject.
- Personal data collected from third parties is permitted with the consent data subjects, their heirs, or their agents.
- The processing of personal data must respect human dignity, privacy and public freedoms.
- Collection of personal data shall be exclusively carried out for lawful and clear purposes.
- Personal data must be processed fairly and to the extent necessary for the purposes for which they were collected.
- The data controller must ensure that the data is accurate and current.
- The processing of personal data may not be carried out for purposes other than those for which they were collected except:
    - if the data subject has given consent;
    - if processing is necessary to safeguard a vital interest of the person concerned; or
    - if processing is necessary for certain scientific purposes.
- Informed consent of the data subject is among the main prerequisites for the legitimate processing of personal data.
- The data subject or their agent may withdraw consent at any time during the processing.
- Personal data relating to children cannot be carried out without the consent of the child's agent and after authorisation of the juvenile and family court judge.
- Consent provided for the processing of personal data under a specific given shall not apply to other forms or purposes.

REGISTRATION AND ENFORCEMENT

The INPDP is authorised to:

- receive and approve requests for personal data processing, and to withdraw such approval;
- receive complaints related to violations of Law No. 2004-63;
- determine the necessary provisions and appropriate measures for the protection of personal data;
- access and verify personal data being processed and collect information necessary to perform their tasks;

- give its opinion on any subject related to the provisions of Law No. 2004-63;
- develop rules of conduct relating to the processing of personal data; and
- participate in research, training and study activities relating to the protection of personal data, and in general to any activity related to its field of intervention.

Any processing of personal data shall be subject to a prior declaration filed at the INPDP headquarters, or by any other means leaving a written record.

CROSS-BORDER TRANSFER

The transfer of personal data is generally prohibited or subject to strict measures, including prior authorisation from the INPDP, and the explicit consent of the person in question, which is mandatory.

The international transfer of personal data is prohibited whenever it may endanger public security or Tunisia's vital interests. Such a transfer may not occur if the foreign country does not provide an adequate level of protection. In every case, the authorisation of the INPDP is required in advance. The INPDP shall issue its decision within one month from the date of receipt of the application.

SECURITY AND BREACH PROTOCOL

Law No. 2004-63 has no stipulated protocol for data breaches.

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