

DATA PROTECTION LAWS OF THE WORLD

Tunisia



Downloaded: 7 August 2024

TUNISIA



Last modified 22 January 2024

LAW

Law n° 2004-63 dated July 27, 2004, on the Protection of Personal Data regulates personal data, but even before that Tunisia was already a pioneer in its region since 2002 in the field of personal data protection. This law was endorsed by the 2022 constitutional embodiment of the protection of privacy, which has placed this protection at the forefront of the rights and freedoms to be guaranteed in the new Republic.

Additionally, articles 56, 61 and 75 of the Organic Law n°2015-26 of August 7, 2015 on the Fight Against Terrorism and the Prohibition of Money Laundering addresses the subject of personal data and when the use of personal data is permitted.

Tunisia became the 51st Member State of the Council of Europe Convention 108 on November 1, 2017 and its Additional Protocol No.181 on supervisory authorities and transborder data flows.

In March 2018, it introduced a new draft law on the protection of personal data in line with the new European GDPR in Parliament, however the law has not yet been passed.

In Tunisia, there is a whole legal arsenal relating to the processing of personal data.

In addition to the above-mentioned texts, there are also decisions rendered by the Instance such as:

- Decision n° 2 of October 6, 2017 on the processing of personal data in the political field;
- Decision n° 3 of September 5, 2018 establishing the countries that represent an adequate level of protection of personal data;
- Decision n° 4 of September 5, 2018 organizing personal health data; and
- Decision n° 5 of September 5, 2018 establishing the conditions and procedures for the installation of cameras and video surveillance.

DEFINITIONS

Definition of personal data

Article 4 of Act n° 2004-63 of July 27, 2004 defined personal data as all information, regardless of their origin or form, and which directly or indirectly, allows to identify or make identifiable, a natural person, with the exception of information related to public life, or considered as such by law.

Definition of sensitive personal data

Act n° 2004-63 of July 27, 2004 did not give a clear definition of sensitive personal data, but it listed some personal data that the processing of which is either prohibited, or would question the data subject's prior consent or the national authority's authorization.

The processing of personal data is prohibited when involving criminal history and proceedings, criminal prosecution, penalties, preventative measures or judicial history.

In addition, the processing of personal data which directly or indirectly concerns the following is also prohibited:

- Racial or genetic origins;
- Religious beliefs;
- Political opinions;
- Philosophical or union activism; or
- Health and scientific research.

Health data is defined by above-mentioned INPDP Decision No. 4 of September 5, 2018 as follows:

“sensitive personal data, which concerns all information related to the physical, mental or psychological health situation of the natural person concerned, as well as his hereditary or acquired genetic characteristics that may characterize him or her and that may result especially from the analysis of a biopsy or physiotherapy services rendered to him or her and that may reveal such information”;

NATIONAL DATA PROTECTION AUTHORITY

The National Authority for Protection of Personal Data (the Instance) was created by Decree n° 2007-3003 of November 27th, 2007. It Has several prerogatives and exercises several control operations that are organized by the decision n° 6 of the Instance dated October 6, 2019.

Any person may file a complaint with the INPDP regarding the violation of personal data committed by any entity.

The decisions of the Instance can be appealed before the Court of Appeal of Tunis and before the Court of Cassation.

REGISTRATION

Any processing of personal data shall be subject to a prior declaration filed at the headquarters of the National Authority for Protection of Personal Data, or by any other means leaving a written record.

- The declaration shall be made by the controller or his legal representative.
- The declaration does not exempt third parties from liability.
- The conditions and procedures for submitting the declaration shall be laid down by decree.
- The Commission may object to the processing of personal data within one month from when the declaration is accepted. (Article 7 of the 2004 Act).

The processing of personal data may be subject to prior authorization by the INDPD if it involves the processing of sensitive personal data, or in the case of transfer of personal data abroad, or if required by law.

The conditions and procedures for obtaining authorization are regulated by Decree n°. 2007-3004 dated 27 November 2007.

DATA PROTECTION OFFICERS

Under Tunisian law (Law n° 2004-63 dated July 27, 2004), there is no reference to Data Protection Officers.

Nevertheless, with regard to health data protection, Decision No. 4 of September 5, 2018 organizing personal health data, healthcare establishments must appoint a DPO.

For other types of sensitive personal data, it is preferable that each entity that processes personal data provides data subjects with an address of its DPO through which they can exercise their right of access to data and their right of opposition to their data processing.

COLLECTION & 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 are permitted whenever the data subject, his heirs or his agent have provided their consent;
- The processing of personal data must respect human dignity, privacy and public liberties, and whatever its origin or its methods, it shall not harm the human rights protected by the laws and the rules in force. In every case, it is forbidden to use personal data with the aim of infringing people's rights or damaging their reputation;
- The collecting of personal data shall be exclusively carried out for lawful and clear purposes, and within the limits of the declared purposes. Any subsequent change of purpose must be the subject of a new declaration and a new consent from the person concerned; and
- Among the main prerequisites for the legitimate processing of personal data is the informed consent of the data subject, which means that the processing of personal data cannot be carried out without the express and written consent of the data subject. This consent shall be governed by the general rules of law if the data subject is incompetent or unauthorized or incompetent to sign.

The data subject or his agent is allowed to withdraw his consent, at any time during the processing.

Additionally, and in the spirit of child protection, Tunisian law has provided extra protection to personal data relating to children as this kind of data cannot be carried out without the consent of the child's agent and after authorization of the juvenile and family court judge.

Finally, the consent provided for the processing of personal data under a specific given shall not apply to other forms or purposes.

Also, the data subject has the right of access, which means the right to consult all the personal data related to him as well as the right to correct, complete, rectify, update, modify, clarify or delete it, when it has been proved that it is inaccurate, equivocal or prohibited for processing by law, and also, the right to obtain a copy of the personal data in clear language, in accordance with the content of the recordings and in an understandable way in the case of automatic processing.

And finally, at anytime, the data subject, his heirs or his tutor has the right to object to the processing of personal data related to him for good, legitimate and serious reasons, except when the processing is scheduled by law or is required by the nature of the commitment. Furthermore, the data subject, his heirs or his tutor have the right to object to the communication to third parties of personal data related to him, in order to exploit it for promotional purpose. The objection immediately suspends the processing.

TRANSFER

The transfer of personal data is treated in the 5th Chapter of the 2004 Act on the protection of personal data (Articles 47 to 52), and is generally prohibited or subject to strict measures, including prior authorization (submitted to the National Authority for Protection of Personal Data), and the explicit consent of the person in question, which is mandatory. The transfer of personal data to a foreign country is prohibited whenever it may endanger public security or Tunisia's vital interests.

The international transfer of personal data may not take occur if the foreign country does not provide an adequate level of protection. In every case, the authorization of the Instance is required before the transfer of personal data. The Instance shall issue its decision within one month from the date of receipt of the application.

In its Decision No. 3 of September 5, 2018, the INPDP issued a non-exhaustive list of countries that represent an adequate level of protection of personal data, and to which the transfer is a priori possible, but always subject to obtaining the authorization of the INPDP.

SECURITY

Each person who carries out directly or by a third party the processing of personal data shall take all the required steps to ensure the safety of the data processing and prevent any third party from changing, modifying or consulting it without prior authorization of the data subject. (article 18 of Organic-Law n°2004-63 of July 27th 2004 on the protection of personal data).

The data controller must ensure that its subcontractor (if any) also implements all the organizational and technical measures necessary to ensure the protection of personal data against any kind of breach.

The National Authority for Protection of Personal Data is responsible for determining the proper measures and necessary safeguards in order to protect personal data.

In case of violation of the personal data protection legislation, in addition to the dissuasive actions it can take, it can also file a complaint with the public prosecutor to initiate criminal action.

If the personal data processed includes sensitive data such as health data, the data controller must subject its processing system to a periodic security audit in accordance with Legislative Decree no. 2023-17 of March 11, 2023 on cybersecurity.

BREACH NOTIFICATION

Under Tunisian Law, it is up to the person in question to make this kind of notification, or to its heirs and agents in certain circumstances.

Mandatory breach notification

The public prosecutor in the jurisdiction where the investigation takes place shall be informed by The National Authority for Protection of Personal Data of any offenses that it has detected.

ENFORCEMENT

The National Authority for Protection of Personal Data is legally mandated to ensure compliance with the provisions of the Law, but there is no information about cases where sanctions were applied to personal data infringements.

A draft bill on personal data has been considered by the Parliamentary Committee on Rights and Freedoms in the former Tunisian Parliament, which revolutionizes the existing Law, and when adopted, will be in correspond to the European standards for Data Protection, the bill has not yet been passed.

ELECTRONIC MARKETING

Electronic Marketing is regulated under Tunisian Law by The Electronic Exchanges and Electronic Commerce Law n° 2000-83 enacted on August 9, 2000.

This law is quite comprehensive and regulates the main aspects of this field. For instance:

- The preservation of the electronic document is as important as the preservation of the written document; and
- Each person using an electronic signature device shall:
 - Take minimum precautions to avoid illegitimate use of encryption elements or personal signature equipment; and
 - Inform the electronic certification service provider of any fraudulent use of his electronic signature.

For matters concerning personal data that have not been regulated by this law, the general protection regime should be applied.

Concerning the exercise of digital advertising, Law n°2004-63 requires the consent of the person concerned. In this context, article 30 of the said Law provides that *it is prohibited to use the processing of personal data for promotional purposes unless the data subject, his heir or his tutor gives his explicit and specific consent. This consent shall be governed by the general rules of law. The provisions of article 28 of the hereby Act shall apply if the data subject is a child*.

ONLINE PRIVACY

There is no specific mention to online privacy under the 2004 law on the Protection of Personal Data.

However, the same safeguards including restrictions and sanctions apply as well to online privacy under Tunisian Law.

Furthermore, it is prohibited to use the processing of personal data for promotional purposes unless the data subject, his heirs or his tutor gives his explicit and specific consent.

KEY CONTACTS



Mohamed Lotfi El Ajeri

Managing Partner

Al Ajeri Lawyers

T +(216) 71 288 251 | 71 287 238

mlelajeri@eal.tn

DATA PRIVACY TOOL

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

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.