DATA PROTECTION LAWS OF THE WORLD

Egypt

EGYPT

Last modified 19 January 2024

LAW

Personal Data Protection Law No.151 of 2020 (the "Law").

DEFINITIONS

Definition of Personal Data

Pursuant to Article (1) of the Law, personal data shall mean any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking such personal data and other data such as name, voice, picture, identification number, online identifier, or any data which determines the psychological, medical, economic, cultural or social identity of a natural person.

Definition of Sensitive Personal Data

Pursuant to Article (1) of the Law, sensitive data shall mean data which discloses psychological, mental or physical health, or genetic, biometric or financial data, religious beliefs, political views, or criminal records. In all cases, data relating to children is considered to be sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Article (19) of the Law, the Personal Data Protection Centre (the "Centre") is a public economic authority that has a legal personality and is under the authority of the Minister of Communications and Information Technology. Such authority aims to protect personal data and regulate the activities of processing and granting access to such personal data. The Centre shall practice all the competences stipulated by the Law for achieving its objectives. Particularly, the Centre has the following competences:

- Setting and developing the policies, strategy plans and the programs necessary for protecting personal data and the execution thereof;
- Unifying the policies and plans for protecting and processing personal data within the Arab Republic of Egypt;
- Setting and applying the decisions, regulations, measures, procedures and criteria related to the protection of personal data;
- Setting a guidance framework for the codes of conduct related to the protection of personal data and approving the codes of conduct of different entities;
- Organizing and cooperating with all the entities, governmental and non-governmental bodies in guaranteeing personal data protection measures and connecting with all the related initiatives;
- Supporting the development of the competence of the personnel working in all governmental and non-governmental entities who are competent with the protection of personal data;

- Issuing licenses, permits, certifications and various measures related to the protection of personal data and the enforcement of the provisions of the Law;
- Accrediting the entities or individuals and granting them the required permits to provide consultation in relation to personal data protection measures;
- Receiving complaints and communications related to the provisions of the Law and issuing the necessary decisions in this regard;
- Advising on draft laws and international agreements which are related to, regulating, or affecting the personal data directly or indirectly;
- Controlling and inspecting the addresses of the provisions of the Law, and take the necessary legal procedures;
- Verifying the conditions of cross-border personal data transfer and issuing the decisions regulating the same;
- Organizing conferences, workshops, training and educational courses and issuing publications to raise awareness and to educate individuals and entities about their rights in relation to dealing with personal data;
- Providing all types of expertise and consultations related to the protection of personal data, in particular to the investigation and judicial authorities;
- Entering into agreements and memoranda of understanding, coordinating cooperating, and knowledge exchange agreements, with international entities, which are relevant to the Centre’s work;
- Issuing circulars which update the personal data protection measures, in accordance with the activities of different sectors and with the Centre’s recommendations; and
- Preparing and issuing an annual report on the status of protection of personal data in the Arab Republic of Egypt.

REGISTRATION

Pursuant to the Law, the controller or the processor must obtain a license or a permit from the Centre for practicing the activity of collecting, storing, transferring, or processing electronic personal data, sensitive data or to undertake any electronic marketing activities.

Applications for licenses, permits, and certifications shall be submitted on the forms produced by the Centre together with all of the supporting documents and information requested to be submitted, along with proof of the applicant's financial ability and its ability to implement the stipulated requirements and technical standards. Decisions on the applications shall be made within a period not exceeding ninety (90) days from the date of completing all documentation and information. The lapse of the above-mentioned period without any decision shall be deemed rejection of the application.

Pursuant to Article (26) of the Law, the licensing fee shall not exceed EGP 2,000,000 (two million Egyptian pounds), while permits or certifications shall not exceed EGP 500,000 (five hundred thousand Egyptian pounds).

DATA PROTECTION OFFICERS

Pursuant to Article (8) of the Law, the legal representative of the juristic person of any of the controller or the processor shall appoint a competent employee as a Data Protection Officer (the “DPO”) within its entity to be responsible for personal data protection. Such DPO must be registered on the DPO register at the Centre. The DPO shall be responsible for enforcing the provisions of the Law and the decisions of the Centre, as well as monitoring and supervising the procedures applicable within the entity and receiving requests related to personal data. The DPO shall, in particular undertake the following:

- Perform a regular evaluation and inspection of the personal data protection systems and avoid infringement thereto as well as documenting the results of such evaluation and issuing the necessary recommendations for its protection.
- Act as a direct contact point with the Centre and implement its decisions, with respect to the application of the provisions of the Law.
- Enable the data subject to practice its rights stipulated under the Law.
- Notify the Centre of the occurrence of any breach of personal data within his entity.
- Reply to the requests submitted by the data subject or any relevant person and reply to the complaints filed by them to the Centre.
- Follow-up the registration and update the personal data records held by the controller, or the processing activity records held by the processor, to guarantee the accuracy of the data and information recorded therein.

- Eliminate any transgressions related to personal data within its entity and undertaking the corrective actions related thereto.
- Organise the necessary training programs for the employees of the relevant legal entity, which are required to have sufficient qualifications that comply with the requirements stipulated by the Law.

COLLECTION & PROCESSING

Data Protection Principles

Controllers and processors must comply with a set of rules governing the processing of personal data. Pursuant to the Law, the following conditions must be fulfilled in order to collect, process and retain personal data:

- Personal data shall be collected for legitimate and specific purposes that shall be disclosed to the data subject.
- Personal data shall be correct, valid, and secured.
- Personal data shall be processed in a legitimate manner and in compliance with the purposes for which it is being collected.
- Personal data shall not be retained for a period longer than that is necessary for the fulfilment of the purpose thereof.

Processing Conditions

Pursuant to Article (6) of the Law, the electronic processing of personal data shall be considered legitimate and legal in cases where it satisfies one of the following conditions:

- It is carried out with the data subject’s consent for the achievement of certain purpose(s);
- It is necessary and intrinsic for the performance of a contractual obligation or legal action, the execution of an agreement for the benefit of the data subject, or the undertaking of any procedure with respect to claiming or defending the data subject's legal rights;
- It is necessary for performing a legal obligation or an order issued by the competent investigation authorities or it is based upon a judicial ruling; or
- It is necessary for enabling the controller to perform its obligations or any relevant person to practice its legitimate rights unless this contradicts the data subject’s fundamental rights and freedoms.

Rights of Data Subjects

Pursuant to Article (2) of the Law, personal data may not be collected, processed, disclosed, or revealed by any means except with the explicit consent of the data subject or where otherwise permitted by law.

Further, the data subjects have a range of rights to control the processing of their personal data, which are as follows:

- To know, review and access / obtain his / her own personal data, which is in possession of any holder, controller or processor;
- To withdraw the prior consent concerning the retention or processing of his/her personal data;
- To correct, edit, erase, add or update his / her personal data;
- To limit the processing to a specified purpose;
- To be notified with any infringement to his / her personal data; and
- To object to the processing of personal data or its results whenever this contradicts the data subject’s fundamental rights and freedoms.

Obligations of the Controller and the Processor:

Pursuant to chapter (3) of the Law, the controller and the processor must comply with certain conditions while collecting and processing personal data, *inter alia*:

- Ensure the validity, conformity and sufficiency of the personal data with the purpose of its collection;

- Not exceed the purpose and period of processing, and notify the controller, the data subject or each relevant person, as the case may be, with the period necessary for processing;
- Set the method, manner, and standards for processing pursuant to the designated purpose;
- Ensure the applicability of the specified purpose for the collection of the personal data for processing objectives;
- Refrain from undertaking any action which would result in disclosing personal data except in the cases permitted by law;
- Adopt all technical and regulatory procedures and apply the necessary standard criteria for protecting personal data and ensuring its confidentiality, and prevent any hack, damage, alteration or manipulation through any illegitimate procedure;
- Correct any error in the personal data immediately upon being notified or becoming aware of such error; and
- Avoid any direct or indirect harm to the data subject.

TRANSFER

Pursuant to Article (14) of the Law, it is prohibited to transfer any personal data that was collected or prepared for processing to a foreign country unless such country grants a level of protection of personal data, that does not fall below what is stipulated in the Law and subject to obtaining a relevant license or permit from the Centre. However, exceptions are made under Article (15) of the Law, if the direct consent of the data subject or his representative is obtained for transferring, sharing, circulating or processing personal data to a country that does not offer the same level of protection in the following cases:

- To protect the data subject’s life and provide them with medical care, treatment, or the administration of medical services.
- To perform obligations in order to prove the existence of a legal right or to exercise or defend such right before the judiciary.
- To conclude or perform an agreement entered into by the person responsible for processing the personal data and third party, which shall be in favor of the concerned data subject.
- To perform a procedure required under an international judicial cooperation.
- There is legal necessity or obligation to protect the public interest.
- To transfer money to another country pursuant to the laws in force of that country.
- If the transfer or circulation is pursuant to a bilateral or multilateral agreement, to which the Arab Republic of Egypt is a party.

In addition, the controller or the processor may, as the case may be, grant access to personal data to another controller or processor outside the Arab Republic of Egypt by virtue of a license from the Centre provided that the following conditions have been met:

- There is conformity between the nature of work of either of the controllers or processors, or unity between the purposes for which they obtain the personal data.
- Either the controllers or processors, or the data subject, have a legitimate interest in the personal data.

The level of legal and technical protection of the personal data offered by the controller or the processor abroad shall not fall below the level of protection provided in the Arab Republic of Egypt.

SECURITY

The Law defines data security as the technological and organizational procedures and operations for the purpose of protecting the privacy, secrecy, safety, unity, and completeness of personal data.

The Law does not state any specific technical standards or measures. However, the Law states that the controller must adopt all technical and regulatory procedures and apply the necessary standard criteria for protecting personal data and to ensure its confidentiality, and prevent any hack, damage, alteration or manipulation through any illegitimate procedure.

Furthermore, Article (25) of the Egyptian Anti-Cybercrimes Law imposes penalties of imprisonment for a period not less than six (6) months and/or a fine not less than EGP 50,000 (fifty thousand Egyptian pounds) and not exceeding EGP 100,000 (one hundred thousand Egyptian pounds). This penalty is imposed regardless of whether the published information is correct or incorrect, on

whoever violates the right to privacy, grants any personal data to a system or a website or sends densified e-mails without the data subject’s consent in order to promote goods or services or to publish information, news, pictures or the like, through the information network or by any means of information technology.

BREACH NOTIFICATION

Pursuant to Article (7) of the Law, each of the controller and the processor, as the case may be, shall notify the Centre with any personal data infringement, within seventy-two (72) hours of such infringement. In the event that such infringement relates to national security protection concerns, the notification shall be immediate. In all events, the Centre shall immediately notify the National Security Authorities with the infringement and provide them, within seventy-two (72) hours from being aware of the infringement, with the following:

- description of the nature of the infringement, the form and the reasons thereof as well as the approximate number of personal data and their records;
- the information of the DPO;
- the potential consequences of the infringement;
- description of the procedures which have been followed and the proposed procedures to be adopted in order to minimize the negative impacts of the infringement;
- evidence of documenting any personal data infringement and the corrective actions which have been taken to solve it; and
- any documents, information or data requested by the Centre.

In all events, the Controller and Processor, as the case may be, shall notify the data subject within three (3) days from the date of notifying the Centre, with the infringement and the adopted procedures related thereto.

The Law defines the National Security Authorities as the Presidency, Ministry of Defence, Ministry of Interior, the General Intelligence Directorate, and the Administrative Control Authority.

ENFORCEMENT

Right to Raise Complaints

Pursuant to Article (33) of the Law, the data subject and any relevant person, has the right to submit a complaint in relation to:

- Infringement or breach of the right of protection of personal data.
- Failure to enable the data subject to exercise his/her rights.
- The decisions issued by the DPO of the processor or controller in relation to the requests submitted to him/her.

Judicial Control Powers

The Centre’s employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Minister of Telecommunications and Information Technology who is the competent minister in this regard, shall have judicial control powers in relation to violations of the Law.

Penalties

Failure to comply with the provisions of the Law, shall be penalized with imprisonment and/or fines that can reach up to EGP 5,000,000 (five million Egyptian pounds).

ELECTRONIC MARKETING

Pursuant to Article (17) of the Law, any electronic communication for the purpose of direct marketing to the data subject shall be prohibited unless the following conditions are met:

- consent is obtained from the data subject;
- the communication includes the identity of its creator and sender;
- the sender has a valid and complete address to be contacted at;

- the purpose is clearly indicated as being for direct marketing; and
- clear and uncomplicated mechanisms are set to allow the data subject to refuse the electronic communication or to withdraw his/her consent to receive such communication.

Further, Article (18) of the Law, provides that the sender of any electronic communication for direct marketing purpose shall undertake to do the following:

- specify a defined marketing purpose;
- not to disclose the contact details of the data subject; and
- maintain electronic records evidencing the consent of the data subject to receive electronic marketing communication and any amendments thereof, or their non-objection to its continuity for a duration of three (3) years from the date of sending the last communication.

ONLINE PRIVACY

The Law does not provide any specific rules for governing cookies and location data. However, pursuant to Article (2) of the Egyptian Anti-Cybercrimes Law No. 175 of 2018, the service providers are under a duty to maintain the privacy of the data stored and not to disclose it to anyone without a reasoned order from a relevant judicial authority. Such duty includes the personal data for any of the users of the service provided by such service provider. A service provider who violates this duty shall be penalized with imprisonment for a period not less than one (1) year and/or a fine not less than EGP 5,000 (five thousand Egyptian pounds) and not exceeding EGP 20,000 (twenty thousand Egyptian pounds).

Furthermore, Article (25) of the Anti-Cybercrimes Law imposes penalties of imprisonment for a period not less than six (6) months and/or a fine not less than EGP 50,000 (fifty thousand Egyptian pounds) and not exceeding EGP 100,000 (one hundred thousand Egyptian pounds). This penalty is imposed regardless of whether the published information is correct or incorrect, on whoever violates the right to privacy, grants any personal data to a system or a website or sends densified e-mails without the data subject’s consent in order to promote goods or services or to publish information, news, pictures or the like, through the information network or by any means of information technology.

KEY CONTACTS

Matouk Bassiouny & Hennawy
matoukbassiouny.com/the-firm/

Nevine Aboualam
Partner
Matouk Bassiouny & Hennawy
T + (202) 2796 2042 (ext.111)
nevine.aboualam@matoukbassiouny.com

DATA PRIVACY TOOL

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