Matouk Bassiouny & Hennawy
matoukbassiouny.com

Law No. 151 of 2020

Promulgating the Personal Data Protection Law

In the Name of the People

The President of the Republic

The House of Representatives has passed the following law and we have promulgated it:

ARTICLE (1)

The provisions of this law and the annexed law shall apply to the protection of personal data processed electronically, in part or in whole, by any holder, controller, or processor in relation to natural persons.

ARTICLE (2)

The provisions of this law and the annexed law shall apply to whoever commits any of the violations stipulated in the annexed law if the offender is an Egyptian residing inside or outside the Arab Republic of Egypt, a non-Egyptian residing inside the Arab Republic of Egypt, or a non-Egyptian outside the Arab Republic of Egypt provided that the act is punishable under any legal form in the country where it occurred, and the data subject of the crime belongs to Egyptians or foreigners residing inside the Arab Republic of Egypt.

ARTICLE (3)

The provisions of the annexed law shall not apply to the following:

1. Personal data of third parties which is held by natural persons and processed for personal use.
2. Personal data which is processed for the purpose of obtaining official statistical data, or in application of a legal provision.
3. Personal data which is processed exclusively for media purposes, provided that it is true and accurate, and not used for any other purpose, without prejudice to the laws governing the press and media.
4. Personal data relating to judicial records, investigations, and lawsuits.
5. Personal data which is held by the national security authorities, and whatever determined by them for other considerations. Upon the request of national security authorities, the Center shall notify the controller or the processor to modify, delete, hide, make available, or circulate personal data within a specified period, according to national security considerations. The controller or processor shall comply with the notification within the specified period therein.
6. Personal data which is held by the Central Bank of Egypt and entities subject to its control and supervision, with the exception of money transfer companies and currency exchange companies, provided that the rules set out by the Central Bank of Egypt in relation to handling personal data are observed.

ARTICLE (4)

The Minister of Telecommunications and Information Technology shall issue the executive regulations of the annexed law (the "**Executive Regulations**") within six (6) months from the effective date of this law.

ARTICLE (5)

The economic courts shall have jurisdiction over committed violations to the provisions of the annexed law.

ARTICLE (6)

The addressees by the provision of this law shall reconcile their positions and comply with the provisions of the annexed law and the Executive Regulations within one (1) year from the date of issuance of the Executive Regulations.

ARTICLE (7)

This law shall be published in the Official Gazette and shall come into force after three (3) months from the following day of its publication.

This law shall be stamped with the seal of the State and be enforced as one of its laws.

Issued at the Presidency on July 13, 2020.

Abdel-Fatah El-Sisi

Matouk Bassiouny & Hennawy
matoukbassiouny.com

Personal Data Protection Law

CHAPTER ONE

Definitions

ARTICLE (1)

In the application of the provisions of this Personal Data Protection Law ("**Law**"), the following terms shall have the meaning ascribed to them:

"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.

"Processing": shall mean any electronic or technological operation to write, collect, record, save, store, merge, display, send, receive, circulate, publish, erase, change, edit, retrieve, or analyze personal data using any electronic or technological medium whether partially or wholly.

"Sensitive Personal 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.

"Data Subject": shall mean any natural person to whom electronically processed personal data is attributed which identifies him/her legally or factually and enable his/her identification from any other person.

"Holder": shall mean any natural or juristic person, legally or factually, holds and retains personal data in any manner, or by any means of storage, regardless of whether that person initially created such personal data or was transferred to such person by any means.

"Controller": shall mean any natural or juristic person who has - by virtue of the nature of their activities - the right to obtain Personal Data and to specify the method and criteria of retaining, Processing or controlling such data according to a specific purpose or to their activities.

"Processor": shall mean any concerned natural or juristic person, by virtue of the nature of its work, to process Personal Data for its own benefit or on behalf of the Controller as agreed with and instructed by the Controller.

"Disclosing Personal Data": shall mean any means which make Personal Data known to others such as by way of viewing, circulating, publishing, transferring, using, displaying, sending, receiving, or disclosing Personal Data.

"Data Security": shall mean technological and organizational procedures and operations the purpose of which is to protect the privacy, secrecy, safety, unity, and completeness of Personal Data.

"Personal Data Infringement": shall mean any unauthorized or illegal access to Personal Data, or any other illegitimate operation to reproduce, send, distribute, exchange, transfer, or circulate which aims to expose or disclose such Personal Data, or damage or edit the same while being stored, transferred or processed.

"Cross-Border Personal Data Transfer": shall mean to transfer, make available, record, store, circulate, publish, use, display, send, receive, retrieve or process Personal Data from inside the Arab Republic of Egypt to outside or vice versa.

"Electronic Marketing": shall mean sending any message, statement, or advertisement or marketing content, via any technological means, which aims, directly or indirectly, to promote goods, services or commercial, political, social, or charitable petitions or requests, addressed to specific persons.

"National Security Authorities": shall mean the Presidency, Ministry of Defense, Ministry of Interior, the General Intelligence Directorate, and the Administrative Control Authority.

"Center": shall mean the Personal Data Protection Center.

"License": shall mean an official document issued by the Center to the juristic person whereby it is granted the right to practice the activity of collecting, storing, transferring, or Processing electronic Personal Data or to undertake Electronic Marketing activities, or all the aforementioned activities and dealing with them in any way. Said document determines the obligations of the licensee in accordance with the rules, conditions, procedures, and technical criteria set out in the Executive Regulations of this Law, and shall be issued for a period of three (3) years, which is renewable for other periods.

"Permit": shall mean an official document issued by the Center to the natural or juristic person whereby it is granted the right to practice the activity of collecting, storing, transferring or Processing electronic Personal Data or to undertake Electronic Marketing activities, or all the aforementioned activities and dealing with them in any way, or to carry out certain task(s). Said document determines the obligations of the permit holder in accordance with the rules, conditions, procedures, and technical criteria set out in the Executive Regulations, and shall be issued for a temporary period not exceeding one (1) year, which may be renewed for more than one period.

"Certification": shall mean a certificate issued from the Center indicating that the natural or juristic person has satisfied all technical, legal, and organizational requirements set out in the Executive Regulations of this Law, whereby it is qualified to provide consultancy services in the field of Personal Data Protection.

"Competent Minister": shall mean the Minister of Telecommunications and Information Technology.

CHAPTER TWO

Rights of the Data Subject and the Conditions for Data Collection and Processing

ARTICLE (2)

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.

The Data Subject shall have the following rights:

1. to know, review and access/ obtain his/her own Personal Data, which is in possession of any Holder, Controller or Processor;
2. to withdraw the prior consent concerning the retention or Processing of his/her Personal Data;
3. to correct, edit, delete, add or update his/her Personal Data;
4. to limit the Processing to a specified purpose;
5. to be notified with any infringement to his/her Personal Data; and
6. to object to the Processing of Personal Data or its results whenever the same contradicts the Data Subject's fundamental rights and freedom.

With exception to item (5) of the above paragraph, the Data Subject shall pay the consideration for the service provided to him/her by the Controller or the Processor with respect to his/her exercise of said rights. The Center shall issue decisions to determine such consideration which shall not exceed EGP 20,000 (twenty thousand Egyptian pounds).

ARTICLE (3)

In order to be able to collect, process, and retain Personal Data, the following conditions must be satisfied:

1. Personal Data shall be collected for legitimate, specific, and transparent purposes to the Data Subject.
2. Personal Data shall be correct, valid, and secured.
3. Personal Data shall be processed in a legitimate manner and in compliance with the purposes for which it is being collected.
4. Personal Data shall not be retained for a period longer than that is necessary for the fulfilment of the purpose thereof.

The Executive Regulations of this Law shall specify the policies, procedures, regulations, and standard criteria for collecting, Processing, storing, and securing of such data.

CHAPTER THREE

Obligations of the Controller and the Processor

First: Controller Obligations

ARTICLE (4)

Without prejudice to Article (12) of this Law, the Controller shall:

1. obtain or receive the Personal Data from the Holder or the competent entities which provide such data, as the case maybe, after obtaining the Data Subject's consent or where otherwise permitted by law;
2. ensure the validity, conformity and sufficiency of the Personal Data with the purpose of its collection;
3. set the method, manner, and standards for Processing pursuant to the designated purpose, unless the Processor has been delegated in this respect by virtue of a written agreement;

4. ensure the applicability of the specified purpose for the collection of the Personal Data for Processing objectives;
5. undertake or refrain from undertaking an action which would result in Disclosing Personal Data except in the cases permitted by law;
6. adopt all technical and regulatory procedures and applying the necessary standard criteria for protecting the Personal Data and ensuring its confidentiality, and preventing any hack, damage, alteration or manipulation through any illegitimate procedure;
7. delete any Personal Data at the Controller's possession upon the satisfaction of the designated purpose. However, in case of retention of such data for any legitimate reason after the satisfaction of its purpose, the data shall be retained in a form that does not allow the identification of the Data Subject;
8. correct any error in the Personal Data immediately upon being notified or aware of such error;
9. maintain record of Personal Data, provided that it shall include the description of the categories of Personal Data in its possession and determining persons to whom such data shall be disclosed or made available along with the basis, duration, restrictions, and scope thereof as well as the mechanisms of deleting or modifying the Personal Data, or any other relevant data related to the Cross-Border Personal Data Transfer. The record shall also include description of the technical and regulatory procedures for Data Security;
10. obtain a License or Permit from the Center to handle Personal Data;
11. Controller outside of the Arab Republic of Egypt is required to appoint a representative in the Arab Republic of Egypt in accordance with the Executive Regulations; and
12. provide the necessary means to prove its abidance with the provisions of this Law and enable the Center to conduct inspections and supervision to ensure the same.

In case there are several Controllers, each Controller shall abide by all the obligations stipulated in this Law, and the Data Subject may exercise his/her rights towards each Controller separately.

The executive regulations shall specify the policies, procedures, regulations, and technical criteria for such obligations.

Second: Processor Obligations

ARTICLE (5)

Without prejudice to Article (12) of this Law, the Processor of Personal Data shall:

1. conduct and implement Processing pursuant to this Law and its Executive Regulation, in accordance with the legitimate and legal cases, and based on the written instructions which are received from the Center, the Controller or from any relevant person as the case may be, and in particular, with respect to the scope, subject and nature of Processing, and the type of Personal Data and its conformity and sufficiency with the designated purpose;
2. ensure the legitimacy of the purpose of Processing and the practice thereof and the non-violation to public order or morals;
3. 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;
4. delete the Personal Data following the lapse of the Processing's period or deliver the same to the Controller;
5. undertake or refrain from undertaking an action, which would result in Disclosing the Personal Data or availability of Processing results except in the cases permitted by law ;
6. not undertake any Processing of Personal Data that contradicts the purpose or the activity of the Controller unless such Processing is for a statistical or educational purpose which shall be not-for-profit and without prejudice to the inviolability of private life;
7. protect and secure the Processing activity and the mediums and the electronic devices used in Processing, as well as the Personal Data thereon;

8. avoid any direct or indirect harm to the Data Subject;
9. prepare a record for the Processing activities, provided that it includes the Processing categories undertaken on behalf of any Controller, its contact details, its Data Protection Officer, the period, restrictions, and scope of Processing, the mechanisms for deleting or modifying the Personal Data, and a description of the technical and organizational procedures related to the Data Security and the Processing activities;
10. provide the means to prove its abidance with the provisions of this Law, upon the request of the Controller, and enable the Center to conduct inspections and supervision to ensure its compliance with the same;
11. obtain a License or a Permit from the Center in order to handle Personal Data; and
12. Processors outside of the Arab Republic of Egypt are required to appoint a representative in the Arab Republic of Egypt in accordance with the Executive Regulations.

In case there are several Processors, each Processor shall abide by all the obligations stipulated under this Law unless there is an agreement setting out the obligations and liabilities of each Processor clearly.

The Executive Regulations shall specify the policies, procedures, regulations, conditions, instructions and standard criteria for such obligations.

Third: Processing Conditions

ARTICLE (6)

Electronic Processing shall be considered legitimate and legal in case it satisfies one of the following conditions:

1. it is carried out upon the Data Subject's consent for the achievement of certain purpose(s);
2. 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;
3. 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
4. It is necessary for enabling the Controller to perform its obligations or any relevant person to practice its legitimate rights unless the same contradicts the Data Subject's fundamental rights and freedom.

Fourth: Obligation to Notify and Inform

ARTICLE (7)

Each of the Controller and the Processor, as the case may be, shall notify the Center 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 Center 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:

1. 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;
2. the information of the Data Protection Officer;
3. the potential consequences of the infringement;
4. 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;
5. evidence of documenting any Personal Data Infringement and the corrective actions which have been taken to solve the same; and

6. any documents, information or data requested by the Center.

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

The Executive Regulations of this Law shall determine the procedures relating to the obligation to notify and inform.

CHAPTER FOUR

Data Protection Officer

First: Data Protection Officer Appointment

ARTICLE (8)

The Center shall set a register for the information of Data Protection Officers. The Executive Regulations shall determine the conditions, procedures and mechanisms of registration.

The legal representative of the juristic person, with respect to any Controller or Processor, shall appoint a competent employee to be responsible for the protection of Personal Data, inside its legal entity and among its personnel structure. Said employee shall be registered in the register designated for the Data Protection Officers at the Center and such appointment shall be announced. ("**Data Protection Officer**")

Controller or Processor who is natural person, shall be the one in-charge of the application of the provisions of this Law.

Second: Data Protection Officer Obligations

ARTICLE (9)

The Data Protection Officer shall be responsible for the application of the provisions of this Law, its Executive Regulations, and the decisions of the Center, as well as supervising and monitoring the applicable procedures within its relevant entity and receiving requests related to Personal Data, according to the provisions of this Law.

The Data Protection Officer shall, in particular, undertake the following:

1. Perform a regular evaluation and inspection of the Personal Data protection systems and avoid infringement thereto and document the results of such evaluation and issue the recommendations necessary for its protection.
2. Act as a point of contact person with the Center and implement its decisions, with respect to the application of the provisions of this Law.
3. Enable the Data Subject to practice the rights stipulated under this Law.
4. Notify the Center with the existence of any Personal Data Infringement.
5. Reply to the requests submitted by the Data Subject or any relevant person and reply to the complaints filed by them to the Center.
6. Follow-up the registration and updating of the Personal Data's record which is maintained by the Controller, or the Processing activities' record which is maintained by the Processor, to guarantee the accuracy of the data and information recorded therein.
7. Eliminate any violations related to Personal Data within its entity and take the corrective actions related thereto.
8. Organize the necessary training programs for the employees within its entity to qualify them in accordance with the requirements of this Law.

The Executive Regulations of this Law shall specify the obligations, procedures, and other tasks that the Data Protection Officer shall perform.

Matouk Bassiouny & Hennawy
matoukbassiouny.com

CHAPTER FIVE

Procedures of Disclosing of Personal Data

ARTICLE (10)

Controller, Processor or Holder shall, whenever it is requested to disclose Personal Data, comply with the following procedures:

1. The request shall be written and submitted by the relevant person or according to a legal deed;
2. Controller, Processor or Holder shall ensure the fulfillment of required documents to grant the access to the Personal Data and retain such documents;
3. The decision regarding the disclosure and its supporting documents shall be made within six (6) working days as of the date of its submission. In case the request is rejected, the decision shall include the rejection's justification. The lapse of the mentioned period without any decision shall be considered a rejection.

ARTICLE (11)

Digital evidence derived from Personal Data pursuant to the provisions of this Law, shall have the same determinative effect of the evidence derived from written data and information, provided that it fulfils the criteria and technical conditions outlined in the Executive Regulations.

CHAPTER SIX

Sensitive Personal Data

ARTICLE (12)

The Controllers and Processors, whether a natural or juristic person, are prohibited from collecting, transferring, storing, saving, Processing or disclosing Sensitive Personal Data except by virtue of a license issued from the Center.

With exception to the cases authorized by law, Controller or Processor must obtain the explicit written consent of the Data Subject.

In case of undertaking any of the above activities in relation to children data, the legal guardian's consent shall be obtained.

The participation of a child in a game, competition or any other activity shall not be conditional on the submission of the child's Personal Data more than what is necessary for participation therein.

The foregoing shall be applied in accordance with the criteria and regulations set out in the Executive Regulation.

ARTICLE (13)

In addition to the obligations mentioned in Article (9) of this Law, the Data Protection Officer of the Controller or the Processor shall follow and implement the security policies and procedures necessary for avoiding any breach or infringement of Sensitive Personal Data.

CHAPTER SEVEN

Cross-Border Personal Data Transfer

ARTICLE (14)

Transfer of Personal Data which is collected or prepared for Processing, to a foreign country, or its storage or sharing may only be undertaken if the level of data protection or security in the foreign country meets (or exceeds) the requirements stipulated under this Law, and subject to obtaining a relevant License or Permit from the Center.

The Executive Regulations of this Law shall set out the policies, criteria, regulations and rules necessary for transferring, storing, sharing, Processing or disclosing Personal Data across borders and the protection thereof.

ARTICLE (15)

Notwithstanding Article (14) of this Law, if the explicit consent of the Data Subject or his representative is obtained, transferring, sharing, circulating or Processing Personal Data may take place without the required minimum protection level stipulated in the previous article, in the following cases:

1. To preserve the life of the Data Subject and provide him/her with medical care or treatment or the management of health services.
2. To perform obligations in order to ensure that a right is proven, exercised or defended before the judiciary.
3. To conclude an agreement or execute an agreement already concluded or, to be concluded, between the Processor and third party, for the benefit of the Data Subject.
4. To perform a procedure relating to international judicial cooperation.
5. There is legal necessity or obligation to protect the public interest.
6. To transfer money to another country pursuant to the laws in force of that country.
7. If the transfer or circulation is pursuant to a bilateral or multilateral international agreement to which Egypt is a party.

ARTICLE (16)

Controller or Processor, as the case may be, may disclose Personal Data to another Controller or Processor outside the Arab Republic of Egypt by virtue of a License from the Center provided that the following conditions are met:

1. if there is conformity between the nature of work of each of the Controllers or Processors, or unity of the purpose for which they obtain the Personal Data;
2. if each of the Controllers, the Processors, or the Data Subject, have a legitimate interest in the Personal Data; and
3. the level of legal and technical protection of the Personal Data provided by the Controller or the Processor abroad shall not be less than the level of protection provided in the Arab Republic of Egypt.

The Executive Regulations of this Law shall determine the necessary conditions, procedures, precautions, criteria, and rules in this regard.

CHAPTER EIGHT

Direct Electronic Marketing

ARTICLE (17)

Any electronic communication for the purpose of direct marketing to the Data Subject shall be prohibited unless the following conditions are met:

1. obtaining the consent of the Data Subject;
2. the communication shall include the identity of the sender;
3. the sender shall have a valid and complete address to be reached;
4. a clear indication that the purpose of communication is for direct marketing; and
5. setting clear and uncomplicated mechanisms to allow the Data Subject to opt-out or withdraw his/her consent in relation thereto.

Article (18)

The sender of any electronic communication for the purpose of direct marketing shall:

1. specify a defined marketing purpose;
2. not disclose the contact details of the Data Subject; and
3. maintain electronic records evidencing the consent of the Data Subject to receive Electronic Marketing communication and any amendments thereof, or his/her non-objection to its continuity for a duration of three (3) years from the date the last communication.

The Executive Regulations shall set forth the necessary rules, conditions, and regulations related to direct Electronic Marketing.

CHAPTER NINE

Personal Data Protection Center

ARTICLE (19)

A public economic authority shall be established under the name of "Personal Data Protection Center" and will be affiliated to the Competent Minister and shall have a juristic personality. Its headquarters shall be located in Cairo or in one of its adjacent governorates. The Center is tasked with the overall mandate of protecting Personal Data and regulating Processing and availability. It shall practice all the competences stipulated under this Law for the purpose of achieving its objectives. Particularly, the Center is responsible for:

- setting and developing the policies, strategic plans, and 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, precautions, 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 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 application of the provisions of this Law;
- Issuing the Certification to entities or individuals and granting them the required permits to provide consultation in relation to Personal Data's protection measures;
- receiving complaints and communications related to the provisions of this 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 addressees of the provisions of this Law and taking 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 in order to raise awareness and to educate individuals and entities on their rights in relation to the 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 exchanging knowledge, with international entities which are relevant to the Center's work, in accordance with the rules and regulations set forth in this regard;
- issuing special patrols to update the Personal Data protection measures, in accordance with the activities of different sectors and with the Center's recommendations; and
- preparing and issuing an annual report on the status of Personal Data protection in the Arab Republic of Egypt.

ARTICLE (20)

The Center shall have a board of directors (the "Board") chaired by the Competent Minister and comprise the membership of each of the following:

1. A representative of the Ministry of Defense appointed by the Minister of Defense;
2. A representative of the Ministry of Interior appointed by the Minister of the Interior;
3. A representative of the General Intelligence Service appointed by the Head of the Agency;
4. A representative of the Administrative Control Authority appointed by the Chairman of the Authority;
5. A representative of the Information Technology Industry Development Agency (ITIDA) appointed by the Chairman of the Board of Directors of the Agency;
6. A representative of the National Telecommunications Regulatory Authority (NTRA) appointed by the Chairman of the Authority;
7. The Center's Chief Executive Officer; and
8. Three (3) experts appointed by the Competent Minister.

The Board's membership tenure shall be three (3) years and renewable. A decree shall be issued by the Prime Minister regarding the formation of the Board and determination of the financial remunerations of the members.

The Board may form amongst its members, one or more committees assigned to them on a temporary basis some tasks. The Board may delegate the Chairman of the Board or the Chief Executive Officer of the Center in some of its competencies.

ARTICLE (21)

The Board of the Center is the dominant authority over its affairs and practice of its competencies. It may take whatever decisions it deems necessary in pursuance of the purposes of the Center, the Law and its Executive Regulations. In particular, the Board may:

- adopt the necessary policies, strategic plans, and programs for the protection of Personal Data;
- approve the regulations, controls, measures, and standards for the protection of Personal Data;
- approve international cooperation and knowledge exchange plans with international entities and organizations;
- approve the organizational structure, the financial, administrative and human resources regulations, and the annual budget of the Center;
- approve the establishment of offices or branches of the Center all over the Arab Republic of Egypt; and
- accept grants, funds, and donations necessary to achieve its purposes after obtaining the approvals required by law.

ARTICLE (22)

The Board of the Center shall meet, upon the invitation of its Chairman, at least once every month, and whenever necessary. The meeting shall be valid in case the majority of board members are attending. Resolutions shall be approved by majority of two-thirds of the attending members. The Chairman may invite any person to attend the meeting without any voting rights.

ARTICLE (23)

The Center shall have Chief Executive Officer (CEO) whose appointment and financial remuneration shall be determined by a decree from the Prime Minister, upon the proposal of the Competent Minister, for a term of four (4) years, renewable for a similar term.

The CEO shall be responsible before the Board for the technical, administrative, and financial works of the Center, and shall represent the Center in its dealings with third parties and before the judiciary. The CEO shall particularly :

1. supervise the implementation of the Board resolutions;
2. manage and supervise the work of the Center, and its affairs;
3. submit periodic reports to the Board on the activity and work progress of the Center, the achievements in accordance with the set objectives, plans, and programs, and the performance obstacles may be encountered and the proposed solutions to avoid them;
4. exercise other competencies determined by the Center's regulations; and
5. take all necessary actions to enforce all the functions and competences of the Center mentioned in Article (21) of this Law.

The CEO shall be assisted by a sufficient number of experts, technicians, and administrative assistants in accordance with the organizational structure of the Center.

ARTICLE (24)

The Board members and employees of the Center are prohibited from disclosing any documents or data relating to cases monitored or examined by the Center, or which are submitted or circulated during the examination or issuance of decisions thereto. This obligation shall remain in force after the termination of the relationship with the Center.

In all cases, the information, documents, and data referred to in this article shall only be disclosed to the investigating authorities and judicial authorities.

ARTICLE (25)

The Center may, in coordination with the competent authorities, cooperate with its counterparts in foreign countries, within the framework of international, regional and bilateral cooperation agreements, ratified cooperation protocols, or in the application of the principle of reciprocity, in order to protect Personal Data and verify the extent of compliance with the law by Controllers and Processors outside Egypt. The Center shall exchange data and information in a manner that shall ensure the protection and non-infringement of Personal Data, as well as assisting in the investigation of violations and relevant crimes and tracking the perpetrators.

CHAPTER TEN

Licenses, Permits, and Certifications

First: Types of Licenses, Permits, and Certifications

ARTICLE (26)

The Center shall issue Licenses, Permits, or Certifications, as follows:

1. The Center shall classify and determine the types of Licenses, Permits, and Certifications, and establish conditions for granting each type thereof, in accordance with the provisions of the Executive Regulations.

2. Issue the License or Permit for Controller or Processor to perform data storing, handling, and Processing activities in accordance with this Law.
3. Issue Licenses or Permits for direct Electronic Marketing.
4. Issue Licenses or Permits for Processing of Personal Data undertaken by associations, unions, or clubs for the members of these entities and in the framework of their activities.
5. Issue Licenses or Permits for means of visual surveillance in public places.
6. Issue Licenses or Permits for the control and Processing of Sensitive Personal Data.
7. Issue Permits and Certifications for individuals and entities to allow them to provide consultancy services on procedures for the protection of Personal Data and compliance procedures.
8. Issue Licenses and Permits for the Cross-Border Personal Data Transfer.

The Executive Regulations shall set out the types, categories, procedures, and conditions of issuance of the Licenses, Permits, Certifications, and the forms used in relation thereto. 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).

Second: Procedures of Issuance of Licenses, Permits and Certifications

ARTICLE (27)

Applications for Licenses, Permits, and Certifications shall be submitted on the forms produced by the Center attaching all 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 mentioned period without any decision shall be deemed rejection of the application.

The Center may request further data, papers, or documents to take a decision in relation to the application. The Center also has the right to request the provision of additional guarantees for the protection of Personal Data in case of insufficiency of the protection mentioned in the submitted documents.

Controller or Processor may obtain more than one License or Permit according to the type of Personal Data.

Third: Amendments of the License and Permit Conditions

ARTICLE (28)

In accordance with public interest considerations, the Center may amend License or Permit conditions after its issuance in any of the following cases:

1. responding to relevant international, regional, or national laws;
2. upon the licensee's request;
3. merger of Controller or Processor with others inside or outside the Arab Republic of Egypt; or
4. amendment is necessary to achieve the objectives of this Law.

Fourth: Cancellation of Licenses, Permits, and Certifications

ARTICLE (29)

The Center may cancel License, Permit or Certification after its issuance in any of the following cases:

1. breach of the License, Permit or Certification;
2. non-payment of the License, Permit or Certification renewal fees;

3. repeated non-compliance with the Center's decisions;
4. assigning the License, Permit or Certification to third party without the Center's approval; or
5. Controller or Processor rendered bankrupted by virtue of judicial ruling.

Fifth: Administrative Sanctions

ARTICLE (30)

Without prejudice to civil and criminal liability provisions under the law, the CEO of the Center shall notify the violator to stop the violation and remove its causes and effects within a specific period. If such period lapses without abiding by the content of the notification, the Board of the Center has the right to issue a reasoned decision with the following:

1. A warning of the partial or total suspension of License, Permit, or Certification for a specific period.
2. Suspension of License, Permit, or Certification in part or in whole.
3. Cancellation or revocation of License, Permit or Certification in part or in whole.
4. Publishing a statement of the violations which have been proven in one or more widespread media means, the cost of which shall be borne by the violator.
5. Subjecting Controller or Processor, as the case may be, to the Center's technical supervision to ensure the protection of Personal Data at its own cost.

CHAPTER 11

Budget and Financial Resources of the Center

ARTICLE (31)

The Center has a special budget that is prepared based on the model of economic authorities in accordance with the rules determined by the Center's regulations and following the rules of the standardized accounting system, without being subject to governmental rules or systems. The Center's fiscal year commences and ends with the State's fiscal year. The Center has its own bank account at the Central Bank of Egypt in which its resources are deposited. The Center may open an account in any commercial bank upon the approval of the Minister of Finance. The Center's budget surplus shall be deferred from a fiscal year to another. Disbursement of the Center's resources shall be made in accordance with the financial regulations and in the areas determined by the Board. The Center's resources of funding consist of the following:

1. its allocated share of the budget of ITIDA;
2. its allocated share, which shall not be less than one-third, of the proceeds of fines imposed in the application of the provisions of this Law;
3. the fees of services provided by the Center;
4. the fees for issuing Licenses, Permits, and Certifications and the reconciliation amounts;
5. the Center's investment revenues; and
6. grants, donations, and gifts accepted by the Board.

CHAPTER 12

Requests and Complaints

First: Requests

ARTICLE (32)

The Data Subject and any relevant person may submit a request to any Holder, Controller or Processor to exercise his/her rights stipulated under this Law and Holder, Controller or Processor is committed to reply within six (6) working days from the date of submission.

Second: Complaints

ARTICLE (33)

Without prejudice to the right to initiate judicial proceedings, the Data Subject and any relevant person, has the right to submit a complaint in any of the following cases:

1. Infringement or breach of the right of Personal Data protection.
2. Failure to enable the Data Subject to exercise his/her rights.
3. The decisions issued by the Data Protection Officer of Processor or Controller in relation to the requests submitted to him/her.

The complaints shall be submitted to the Center who has the right to take the necessary investigative actions. The decision of the Center shall be issued within thirty (30) working days from the date of submission. The complainant and the respondent shall be notified with the decision.

The respondent shall execute the Center's decision within seven (7) working days from the notification date and notify the Center of such execution.

CHAPTER 13

Judicial Control

ARTICLE (34)

The Center's employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Competent Minister, shall have judicial control powers in relation to violations of this Law.

CHAPTER 14

Crimes and Penalties

ARTICLE (35)

Without prejudice to any severer sanctions stipulated under any other law and without prejudice to the injured party's right to seek damages, the crimes set forth in the following Articles shall be penalized with the following penalties.

ARTICLE (36)

Holders, Controllers and Processors who collect, process, disclose, make available, or circulate Personal Data that has been electronically processed in cases that have not been authorized by the law or without the consent of the data subject, shall be penalized with a fine not less than EGP 100,000 (One Hundred Thousand Egyptian Pounds) and not exceeding EGP 1,000,000 (One Million Egyptian Pounds).

However, if this is committed in exchange for a material or moral benefit or to endanger or harm the Data Subject, the Penalty shall be imprisonment for a period not less than six (6) months, and/or a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds) and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

(ARTICLE 37)

Holders, Controllers and Processors who refrained without legal justification, from enabling the Data Subject to exercise his/her rights, stipulated under Article (2) of this Law, shall be penalized with a fine not less than EGP 1,000,000 (One Hundred Thousand Egyptian Pounds) and not exceeding EGP 1,000,000 (One Million Egyptian Pounds). Further, whoever collect Personal Data without complying with provisions stipulated under Article (3) of this Law shall be penalized with a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds) and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

ARTICLE (38)

Controllers and Processors who do not perform their obligations under Articles (4), (5) and, (7) of this Law shall be penalized with a fine not less than EGP 300,000 (Three Hundred Thousand Egyptian Pounds) and not exceeding EGP 3,000,000 (Three Million Egyptian Pounds).

ARTICLE (39)

The legal representatives of juristic persons who do not fulfill their obligations under Article (8) of this Law shall be penalized with a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds) and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

ARTICLE (40)

Data Protection Officers who fail to carry out their duties stipulated under Article (9) of this Law shall be penalized with a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds) and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

If a violation occurs due to negligence of the Data Protection Officer, the penalty shall be a fine not less than EGP 50,000 (Fifty Thousand Egyptian Pounds) and not exceeding EGP 500,000 (Five Hundred Thousand Egyptian Pounds).

ARTICLE (41)

Holders, Controllers and Processors who collect, make available, circulate, Process, disclose, store, transfer or save Sensitive Personal Data without the consent of the Data Subject or in cases that have not been permitted by law, shall be sentenced to imprisonment for a period not less than three (3) months and/or a fine not less than EGP 500,000 (Five Hundred Thousand Egyptian Pounds) and not exceeding EGP 5,000,000 (Five Million Egyptian Pounds).

ARTICLE (42)

Whoever violates the conditions of Cross-Border Personal Data Transfer stipulated under Articles (14), (15), and (16) shall be sentenced to imprisonment for a period not less than three (3) months and/or a fine not less than EGP 500,000 (Five Hundred Thousand Egyptian Pounds) and not exceeding EGP 5,000,000 (Five Million Egyptian Pounds).

ARTICLE (43)

Whoever violates the Electronic Marketing provisions stipulated under Articles (17) and (18) of this Law shall be penalized by a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds)and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

ARTICLE (44)

Members of the Board of the Center and its employees who violate the obligations stipulated under Article (24) of this Law shall be penalized by a fine not less than EGP 300,000 (Three Hundred Thousand Egyptian pounds) and not exceeding 3,000,000 (Three Million Egyptian Pounds).

ARTICLE (45)

Whoever violates the provisions of Licenses, Permits, or Certifications stipulated under this Law shall be penalized with a fine not less than EGP 500,000 (Five Hundred Thousand Egyptian Pounds) and not exceeding EGP 5,000,000 (Five Million Egyptian Pounds).

ARTICLE (46)

Whoever prevents any of the Center's employees who have control powers from performing their work shall be sentenced to imprisonment for a period not less than six (6) months and/or a fine not less than EGP 200,000 (Two Hundred Thousand Egyptian Pounds) and not exceeding EGP 2,000,000 (Two Million Egyptian Pounds).

ARTICLE (47)

The de facto manager of the violating juristic person shall be penalized with the same sanctions stipulated for violations of this Law, if it is proven that the manager knew about the violation and if his breach of the duties imposed by the juristic person contributed to the violation.

The juristic person shall be jointly responsible for the payment of damages, if the violation is committed by one of its employees, under the juristic person's name and for its account and benefit.

ARTICLE (48)

In all cases, and in addition to penalties set forth under this Law, the courts order that the sentences be published in two widespread newspapers and on the internet at the expense of the convict.

In case of recidivism, the sanctions stipulated in this chapter will be doubled with their minimum and maximum limits.

The attempt to commit violations under this Law shall be sanctioned with half the prescribed penalties.

Settlement and Reconciliation

ARTICLE (49)

At any stage of the criminal proceedings and before the issuance of a final judgment, the defendant may evidence the settlement with the claimant, its representative or successor and upon the Center's approval before the Public Prosecutor's Office or the competent court, as the case may be, in respect of the misdemeanors stipulated under Articles (36), (37), (38), (39), (40), (41) and (43) of this Law.

Reconciliation with relation to the misdemeanors stipulated under Articles (42), (44) and (45) of this Law may be reached with the Center at any stage of the proceedings.

In all cases, the defendant who seeks reconciliation, shall pay before the initiation of criminal proceedings, an amount equivalent to half of minimum fine set forth for the violation.

The defendant who seeks settlement after the initiation of criminal proceedings and before the issuance of a final judgment, shall pay half of the maximum fine set forth for the violation or the adjudicated fine, whichever is higher.

The payment shall be made to the competent court's treasury, the Public Prosecutor's Office, or the Center, as the case may be.

Reconciliation entails the lapse of criminal proceedings without any effect on the rights of the injured party from the violation.