UNOFFICIAL ENGLISH TRANSLATION

Prepared by Youssry Saleh & Partners

Law No. 151 of 2020

Promulgating the Personal Data Protection Law

17 August 2026

This unofficial English translation has been prepared by Youssry Saleh & Partners for information and accessibility. It does not replace the Arabic text published in the Official Gazette. In the event of any discrepancy, the official Arabic text prevails.

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, which We hereby promulgate:

Article 1

The provisions of this Law and the Attached Law apply to the protection of Personal Data relating to natural persons where those data are processed electronically, wholly or partly, by any Holder, Controller or Processor.

Article 2

The provisions of this Law and the Attached Law apply to any person who commits any of the offences provided for in the Attached Law if the offender is an Egyptian national, whether within or outside the Republic; is a non-Egyptian residing within the Republic; or is a non-Egyptian outside the Republic, provided that the act is punishable in the State in which it occurred under any legal characterisation and the data that are the subject of the offence relate to Egyptians or to foreign nationals residing within the Republic.

Article 3

The provisions of the Attached Law do not apply to:

1. Personal Data kept by natural persons for others and Processed for personal use.
2. Personal Data Processed for the purpose of obtaining official statistical data or in application of a statutory provision.
3. Personal Data Processed exclusively for media purposes, provided that they are correct and accurate and are not used for any other purpose, without prejudice to the legislation regulating the press and media.
4. Personal Data relating to judicial enforcement records, investigations and court proceedings.
5. Personal Data held by the National Security Authorities, and any other data that those Authorities determine should be excluded for other considerations. At the request of the National Security Authorities, the Center must notify the Controller or Processor to modify or erase Personal Data, or not to display, make available or circulate them, within a specified period and in accordance with national security considerations. The Controller or Processor must implement the notification within the period specified in it.
6. Personal Data held by the Central Bank of Egypt and entities subject to its control and supervision, except money transfer companies and foreign exchange companies, in respect of which the rules established by the Central Bank of Egypt for handling Personal Data must be observed.

Article 4

The Minister responsible for communications and information technology must issue the Executive Regulations of the Attached Law within six months from the date on which this Law comes into force.

Article 5

The Economic Courts have jurisdiction over offences committed in contravention of the provisions of the Attached Law.

Article 6

Persons subject to this Law must bring their affairs into compliance with the Attached Law and its Executive Regulations within one year from the date on which those Regulations are issued.

Article 7

This Law must be published in the Official Gazette and comes into force after three months have elapsed from the day following the date of its publication.

This Law must be stamped with the Seal of the State and enforced as one of its laws.

Issued at the Presidency of the Republic on 22 Dhu al-Qi'dah 1441 AH

(corresponding to 13 July 2020 AD).

Abdel Fattah El-Sisi

Personal Data Protection Law

Chapter One
Definitions

Article 1

For the purposes of this Law, the following words and expressions have the meanings given to them below:

Personal Data means any data relating to an identified natural person or to a natural person who can be identified, directly or indirectly, by linking those data with any other data, such as a name, voice, image, identification number, online identifier, or any data identifying the person's psychological, health, economic, cultural or social identity.

Processing means any electronic or technical operation involving writing, collecting, recording, keeping, storing, combining, displaying, sending, receiving, circulating, publishing, erasing, changing, modifying, retrieving or analysing Personal Data using any electronic or technical medium or device, whether the operation is carried out wholly or partly.

Sensitive Personal Data means data that disclose psychological, mental, physical or genetic health, biometric measurement data, financial data, religious beliefs, political opinions or security status. In all cases, children's data are considered Sensitive Personal Data.

Data Subject means any natural person to whom electronically Processed Personal Data are attributed, where those data identify the person in law or in fact and enable the person to be distinguished from others.

Holder means any natural or legal person who, in law or in fact, possesses and retains Personal Data in any form or on any storage medium, whether that person created the data or came into possession of them in any manner.

Controller means any natural or legal person who, by virtue of that person's work or the nature of that work, has the right to obtain Personal Data and to determine the method, manner and criteria for retaining them, or for Processing them and exercising control over them, in accordance with the specified purpose or that person's activity.

Processor means any natural or legal person who, by the nature of that person's work, specialises in Processing Personal Data for that person's own benefit or for the benefit of a Controller under an agreement with, and in accordance with the instructions of, that Controller.

Making Personal Data Available means any means by which another person is made aware of Personal Data, such as viewing, circulation, publication, transfer, use, display, sending, receipt or disclosure.

Data Security means technical and organisational procedures and operations for preserving the privacy and confidentiality of Personal Data, their integrity and unity, and their integration with one another.

Personal Data Breach and Violation means any unauthorised entry into Personal Data or unlawful access to them, or any unlawful operation involving the copying, sending, distribution, exchange, transfer or circulation of Personal Data, where that operation is intended to reveal or disclose those data, or to destroy or modify them, while they are being stored, transferred or Processed.

Cross-Border Movement of Personal Data means transferring, making available, recording, storing, circulating, publishing, using, displaying, sending, receiving, retrieving or Processing Personal Data from within the geographical territory of the Arab Republic of Egypt to outside that territory, or vice versa.

Electronic Marketing means the sending, by any technical means whatever its nature or form, of any message, statement or advertising or marketing content intended, directly or indirectly, to promote goods or services or commercial, political, social or charitable solicitations or requests directed to particular persons.

National Security Authorities means the Presidency of the Republic, the Ministry of Defense, the Ministry of Interior, the General Intelligence Service and the Administrative Control Authority.

Center means the Personal Data Protection Center.

Licence means an official document issued by the Center to a legal person, granting that person the right to carry on the activity of collecting, storing, transferring or Processing electronic Personal Data; to conduct Electronic Marketing activities; or to carry on all of those activities and deal with the data in any manner. The document specifies the licensee's obligations in accordance with the rules, conditions, procedures and technical standards prescribed by the Executive Regulations of this Law. It is valid for three years and may be renewed for further periods.

Permit means an official document issued by the Center to a natural or legal person, granting that person the right to carry on the activity of collecting, storing, transferring or Processing electronic Personal Data; to conduct Electronic Marketing activities; to carry on all of those activities and deal with the data in any manner; or to perform one or more specified tasks. The document specifies the permit holder's obligations in accordance with the rules, conditions, procedures and technical standards prescribed by the Executive Regulations. It is valid for a temporary period not exceeding one year and may be renewed more than once.

Accreditation means a certificate issued by the Center stating that a natural or legal person has met all the technical, legal and organisational requirements prescribed by the Executive Regulations of this Law and is, by virtue of that certificate, qualified to provide consultancy services in the field of Personal Data protection.

Competent Minister means the minister responsible for communications and information technology.

Chapter Two
Rights of the Data Subject and Conditions for Collecting and Processing Data

Article 2

Personal Data must not be collected, Processed, disclosed or divulged by any means without the Data Subject's express consent, except where authorised by law.

The Data Subject has the following rights:

1. to be informed of the Personal Data relating to them that are held by any Holder, Controller or Processor, to inspect those data and to access or obtain them;
2. to withdraw their prior consent to the retention or Processing of their Personal Data;
3. to have their Personal Data corrected, modified, erased, supplemented or updated;
4. to have Processing limited to a specified scope;
5. to be informed of any breach or violation affecting their Personal Data; and
6. to object to the Processing of Personal Data or to its results where that Processing or those results conflict with the Data Subject's fundamental rights and freedoms.

Except in relation to the right in item (5) of the preceding paragraph, the Data Subject must pay the cost of the service provided to them by the Controller or Processor in connection with the exercise of their rights. The Center must issue decisions determining that amount, which must not exceed twenty thousand Egyptian pounds.

Article 3

The following conditions must be met in the collection, Processing and retention of Personal Data:

1. the Personal Data must be collected for lawful, specified purposes that have been made known to the Data Subject;
2. the Personal Data must be accurate, sound and secure;
3. the Personal Data must be Processed in a lawful manner appropriate to the purposes for which they were collected; and
4. the Personal Data must not be retained for longer than is necessary to fulfil the purpose specified for them.

The Executive Regulations of this Law must specify the policies, procedures, controls and standards for collecting, Processing, keeping and securing those data.

Chapter Three
Obligations of the Controller and Processor

First: Obligations of the Controller

Article 4

Without prejudice to Article 12 of this Law, the Controller must:

1. obtain or receive Personal Data from the Holder or from the competent entities responsible for supplying them, as applicable, after obtaining the Data Subject's consent or in cases authorised by law;
2. ensure the accuracy of Personal Data and their consistency with, and adequacy for, the specified purpose for which they are collected;
3. establish the method, manner and standards of Processing in accordance with the specified purpose, unless the Controller decides to delegate that task to the Processor under a written contract;
4. ensure that the Processing of Personal Data is consistent with the specified purpose for which they were collected;
5. not, by any act or omission, make Personal Data Available except in cases authorised by law;
6. take all technical and organisational measures and apply the standards necessary to protect and secure Personal Data, preserve their confidentiality, and prevent their breach, destruction, alteration or tampering through any unlawful operation;
7. erase Personal Data held by it immediately upon expiry of their specified purpose. If they are retained for any lawful reason after that purpose has ended, they must not remain in a form that permits the Data Subject to be identified;
8. correct any error in Personal Data immediately upon being notified of it or becoming aware of it;
9. maintain a dedicated data record which includes a description of the categories of Personal Data held by it; the persons to whom those data are to be disclosed or made available; the legal basis for doing so; the relevant periods and their restrictions and scope; the mechanisms for erasing or modifying Personal Data held by it; any other information relating to the cross-border transfer of those Personal Data; and a description of the technical and organisational measures for Data Security;
10. obtain a Licence or Permit from the Center for handling Personal Data;
11. if it is outside the Arab Republic of Egypt, appoint a representative in the Arab Republic of Egypt in the manner specified by the Executive Regulations; and
12. provide the facilities necessary to demonstrate its compliance with this Law and enable the Center to conduct inspections and exercise supervision to verify that compliance.

Where there is more than one Controller, each Controller must comply with all the obligations provided for in this Law, and the Data Subject may exercise their rights against each Controller separately.

The Executive Regulations of this Law must specify the policies, procedures, controls and technical standards applicable to those obligations.

Second: Obligations of the Processor

Article 5

Without prejudice to Article 12 of this Law, the Processor must:

1. undertake and carry out Processing in accordance with the rules governing it under this Law and its Executive Regulations, in legitimate and lawful circumstances, and on the basis of written instructions received from the Center, the Controller or any person entitled to issue them, as applicable, particularly as regards the scope, subject matter and nature of the Processing, the type of Personal Data, and their consistency with, and adequacy for, the specified purpose;
2. ensure that the purposes and conduct of Processing are legitimate and do not contravene public order or public morals;
3. not exceed the specified purpose or duration of Processing, and notify the Controller, the Data Subject or any other person entitled to be notified, as applicable, of the period necessary for Processing;
4. erase Personal Data upon expiry of the Processing period or deliver them to the Controller;
5. not, by any act or omission, make Personal Data or the results of Processing available except in cases authorised by law;
6. not carry out any Processing of Personal Data that is inconsistent with the Controller's purpose or activity, unless the Processing is for a statistical or educational purpose, is not intended for profit and does not infringe the inviolability of private life;
7. protect and secure the Processing operation, the media and electronic devices used for it, and the Personal Data held on them;
8. not cause the Data Subject any direct or indirect harm;
9. maintain a dedicated record of its Processing operations which includes the categories of Processing it carries out on behalf of each Controller; the Controller's contact details and the details of its Data Protection Officer; the periods, restrictions and scope of Processing; the mechanisms for erasing or modifying Personal Data held by it; and a description of the technical and organisational measures for the security of the data and Processing operations;
10. provide the facilities necessary to demonstrate its compliance with this Law when requested by the Controller, and enable the Center to conduct inspections and exercise supervision to verify its compliance;
11. obtain a Licence or Permit from the Center for handling Personal Data; and
12. if it is outside the Arab Republic of Egypt, appoint a representative in the Arab Republic of Egypt in the manner specified by the Executive Regulations.

Where there is more than one Processor and no contract clearly defines the obligations and responsibilities of each, every Processor must comply with all the obligations provided for in this Law.

The Executive Regulations of this Law must specify the policies, procedures, controls, conditions, instructions and standards applicable to those obligations.

Third: Conditions for Processing

Article 6

Electronic Processing is considered legitimate and lawful if any of the following applies:

1. the Data Subject consents to the Processing for one or more specified purposes;
2. the Processing is necessary and indispensable for the performance of a contractual obligation or legal act, for the conclusion of a contract for the benefit of the Data Subject, or for taking any step to assert or defend the Data Subject's legal rights;
3. it is undertaken to perform an obligation regulated by law, comply with an order of the competent investigating authorities, or give effect to a court judgment; or
4. it enables the Controller to perform its obligations or a person with standing to exercise their legitimate rights, unless this conflicts with the Data Subject's fundamental rights and freedoms.

Fourth: Obligation to Notify and Report

Article 7

When a Controller or Processor, as applicable, becomes aware of a breach or violation of Personal Data held by it, it must report the breach or violation to the Center within seventy-two hours. If the breach or violation relates to considerations concerning the protection of national security, the report must be made immediately. In all cases, the Center must immediately notify the National Security Authorities of the incident. The Controller or Processor must also provide the Center, within seventy-two hours from becoming aware of the incident, with:

1. a description of the nature, form and causes of the breach or violation, the approximate volume of Personal Data concerned and the number of related records;
2. details of its Data Protection Officer;
3. the likely effects of the breach or violation;
4. a description of the measures taken and proposed to address the breach or violation and mitigate its adverse effects;
5. documentation of the breach or violation and the corrective measures taken to address it; and
6. any documents, information or data requested by the Center.

In all cases, the Controller or Processor, as applicable, must notify the Data Subject within three working days from the date on which the report is made and inform the Data Subject of the measures taken.

The Executive Regulations of this Law must specify the procedures for reporting and notification.

Chapter Four
Data Protection Officer

First: Appointment of the Data Protection Officer

Article 8

A register of Data Protection Officers is established at the Center. The Executive Regulations of this Law must specify the conditions and procedures for entry in the register and the registration mechanisms.

The legal representative of a Controller or Processor that is a legal person must appoint, within that legal person's organisational and staffing structure, a specialised employee responsible for Personal Data protection, register that employee in the Center's register of Data Protection Officers, and publicly announce the appointment.

A Controller or Processor that is a natural person is responsible for implementing this Law.

Second: Obligations of the Data Protection Officer

Article 9

The Data Protection Officer is responsible for implementing this Law, its Executive Regulations and the Center's decisions; monitoring and supervising the procedures applied within the officer's entity; and receiving requests relating to Personal Data in accordance with this Law. In particular, the officer must:

1. periodically assess and examine systems for protecting Personal Data and preventing breaches of those systems, document the assessment results and issue the recommendations necessary to protect those systems;
2. act as a direct point of contact with the Center and implement its decisions concerning the application of this Law;
3. enable the Data Subject to exercise the rights provided for in this Law;
4. notify the Center of any breach or violation of Personal Data held by the officer's entity;
5. respond to requests submitted by the Data Subject or any other person entitled to make the request, and respond to the Center concerning grievances submitted to the Center by either of them, in accordance with this Law;
6. monitor entries in, and updates to, the Controller's Personal Data record or the Processor's record of Processing operations, so as to ensure the accuracy of the data and information recorded in the relevant record;
7. remedy any violations relating to Personal Data within the officer's entity and take corrective measures in respect of them; and
8. organise the training programmes necessary to equip the entity's employees in a manner appropriate to the requirements of this Law.

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

Chapter Five
Procedures for Making Personal Data Available

Article 10

When requested to make Personal Data Available, a Controller, Processor or Holder must:

1. act only on a written request submitted by a person entitled to make the request or pursuant to a legal basis;
2. verify that the documents necessary for Making Personal Data Available are present and retain those documents; and
3. determine the request, together with its supporting documents, within six working days from the date on which the request is submitted. A decision rejecting the request must state the reasons for rejection. If that period expires without a response, the request is deemed to have been rejected.

Article 11

Digital evidence derived from Personal Data in accordance with this Law has the same probative force as evidence derived from written data and information, provided that it meets the standards and technical conditions specified in the Executive Regulations of this Law.

Chapter Six
Sensitive Personal Data

Article 12

A Controller or Processor, whether a natural person or a legal person, must not collect, transfer, store, keep, Process or make Sensitive Personal Data available except under a Licence issued by the Center. Except in cases authorised by law, the Data Subject's express written consent must be obtained. Where any of those operations concerns children's data, the consent of the child's guardian must be obtained.

A child's participation in a game, competition or any other activity must not be conditional on the provision of Personal Data relating to the child beyond what is necessary for that participation.

All the foregoing is subject to the standards and controls specified by the Executive Regulations of this Law.

Article 13

In addition to the obligations set out in Article 9 of this Law, the Data Protection Officer and the staff under that officer's supervision at the Controller or Processor must comply fully with the security policies and procedures necessary to prevent Sensitive Personal Data from being breached or violated.

Chapter Seven
Personal Data Across Borders

Article 14

Personal Data that have been collected or prepared for Processing must not be transferred to a foreign State, or stored or shared in a foreign State, unless a level of protection no lower than that provided for in this Law is available and a Licence or Permit has been obtained from the Center.

The Executive Regulations of this Law must specify the policies, standards, controls and rules necessary for transferring, storing, sharing, Processing or Making Personal Data Available across borders, and for protecting those data.

Article 15

By way of exception to Article 14 of this Law, where the express consent of the Data Subject or the Data Subject's representative has been obtained, Personal Data may be transferred to a State that does not provide the level of protection referred to in the preceding Article, or shared, circulated or Processed in that State, in any of the following cases:

1. preserving the life of the Data Subject and providing the Data Subject with medical care, treatment or the management of health services;
2. performing obligations in a manner that enables a right to be established, exercised before the authorities responsible for the administration of justice, or defended;
3. the conclusion of a contract, the performance of a contract already concluded, or the future conclusion of a contract between the person responsible for Processing and a third party, for the benefit of the Data Subject;
4. carrying out a procedure relating to international judicial cooperation;
5. where it is necessary, or there is a legal obligation, to protect the public interest;
6. making money transfers to another State in accordance with the applicable legislation in force in that State; or
7. where the transfer or circulation is effected pursuant to a bilateral or multilateral international agreement to which the Arab Republic of Egypt is a party.

Article 16

A Controller or Processor may, as applicable, make Personal Data Available to another Controller or Processor outside the Arab Republic of Egypt under a Licence from the Center if:

1. the nature of the activities of the two Controllers or Processors is compatible, or the purpose for which they obtain the Personal Data is the same;
2. each of the Controllers or Processors of the Personal Data, or the Data Subject, has a legitimate interest; and
3. the level of legal and technical protection for Personal Data held abroad by the Controller or Processor is no lower than the level available in the Arab Republic of Egypt.

The Executive Regulations of this Law must specify the conditions, procedures, safeguards, standards and rules necessary for this purpose.

Chapter Eight
Direct Electronic Marketing

Article 17

An electronic communication for the purpose of direct marketing to a Data Subject must not be made unless:

1. the Data Subject's consent has been obtained;
2. the communication identifies its originator and sender;
3. the sender has a valid and sufficient address at which the sender can be reached;
4. the communication indicates that it is sent for direct marketing purposes; and
5. clear and accessible mechanisms are provided to enable the Data Subject to reject the electronic communication or withdraw consent to its being sent.

Article 18

The sender of an electronic communication for the purpose of direct marketing must:

1. adhere to the specified marketing purpose;
2. not disclose the Data Subject's contact details; and
3. retain, for three years from the date of the last transmission, electronic records evidencing the Data Subject's consent and any amendments to it, or the Data Subject's lack of objection to continuing to receive the Electronic Marketing communication.

The Executive Regulations of this Law must specify the rules, conditions and controls relating to direct Electronic Marketing.

Chapter Nine
Personal Data Protection Center

Article 19

A public economic authority named the "Personal Data Protection Center" is established. It is subordinate to the Competent Minister and has legal personality. Its principal office is situated in Cairo Governorate or one of the neighbouring governorates. Its purpose is to protect Personal Data and regulate the Processing and Making Available of Personal Data. To achieve its purposes, the Center may exercise all the functions provided for in this Law and, in particular, may:

formulate and develop the policies, strategic plans and programmes necessary for the protection of Personal Data, and oversee their implementation;

unify policies and plans for the protection and Processing of Personal Data throughout the Republic;

formulate and implement the decisions, controls, measures, procedures and standards relating to the protection of Personal Data;

establish a guidance framework for codes of conduct concerning the protection of Personal Data, and approve the Personal Data protection codes of conduct of different entities;

coordinate and cooperate with all governmental and non-governmental entities and agencies to ensure Personal Data protection procedures, and communicate with all related initiatives;

support capacity-building for personnel working in all governmental and non-governmental entities responsible for the protection of Personal Data;

issue Licences, Permits, approvals and other measures relating to the protection of Personal Data and the application of this Law;

accredit entities and individuals and grant them the necessary Permits enabling them to provide consultancy services concerning Personal Data protection procedures;

receive complaints and reports relating to this Law and issue the necessary decisions concerning them;

express an opinion on draft laws and international agreements that regulate or relate to Personal Data, or whose provisions have a direct or indirect bearing on them;

monitor and inspect persons subject to this Law and take the necessary legal measures;

verify the conditions governing Cross-Border Movement of Personal Data and issue decisions regulating it;

organise conferences, workshops and training and educational courses, and publish materials to raise awareness and educate individuals and entities about their rights in relation to dealing with Personal Data;

provide all forms of expertise and consultancy relating to the protection of Personal Data, particularly to investigative authorities and judicial bodies;

enter into agreements and memoranda of understanding with international bodies whose work relates to that of the Center, and coordinate, cooperate and exchange expertise with those bodies, in accordance with the rules and procedures prescribed in that regard;

publish periodicals on updates to protection procedures that are compatible with the activities of the different sectors and with the Center's recommendations in that regard; and

prepare and issue an annual report on the state of Personal Data protection in the Arab Republic of Egypt.

Article 20

The Center has a Board of Directors chaired by the Competent Minister and comprising:

1. a representative of the Ministry of Defense, selected by the Minister of Defense;
2. a representative of the Ministry of Interior, selected by the Minister of Interior;
3. a representative of the General Intelligence Service, selected by the Head of the Service;
4. a representative of the Administrative Control Authority, selected by the Chair of the Authority;
5. a representative of the Information Technology Industry Development Agency, selected by the Chair of the Agency's Board of Directors;

6. a representative of the National Telecom Regulatory Authority, selected by the Chair of the Authority's Board of Directors;

7. the Chief Executive Officer of the Center; and

8. three persons with expertise, selected by the Competent Minister.

Membership of the Board of Directors is for a term of three years, which may be renewed. The Board of Directors is constituted, and the financial terms of its members are determined, by a decision of the Prime Minister.

The Board of Directors may form one or more committees from among its members and temporarily entrust them with certain tasks. It may delegate some of its functions to the Chair of the Board of Directors or the Chief Executive Officer of the Center.

Article 21

The Center's Board of Directors is the authority having overall control over its affairs and the exercise of its functions. It may adopt any decisions it considers necessary to achieve the purposes of the Center, this Law and its Executive Regulations and, in particular, may:

approve the policies, strategic plans and programmes necessary for the protection of Personal Data;

approve the regulations, controls, measures and standards concerning the protection of Personal Data;

approve plans for international cooperation and the exchange of expertise with international entities and organisations;

approve the organisational 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 throughout the Republic; and

accept grants, donations and gifts necessary to achieve the purposes of the Center, after obtaining the approvals required by law.

Article 22

The Center's Board of Directors must meet when convened by its Chair at least once every month and whenever necessary. A meeting is valid if a majority of its members are present. Its decisions must be adopted by a two-thirds majority of the votes of the members present. The Chair may invite any person to attend a meeting, but that person has no vote.

Article 23

The Center has a Chief Executive Officer. The Chief Executive Officer is appointed, and the financial terms of the appointment are determined, by a decision of the Prime Minister on the proposal of the Competent Minister. The appointment is for a term of four years and may be renewed once.

The Chief Executive Officer is responsible to the Board of Directors for the technical, administrative and financial conduct of the Center's work and represents the Center in its relations with third parties and before the courts. The Chief Executive Officer has the following functions in particular:

1. supervising the implementation of the decisions of the Board of Directors;
2. managing the Center, supervising the conduct of its work and administering its affairs;
3. submitting periodic reports to the Board of Directors on the Center's activities, the conduct of its work and what has been achieved in accordance with the established objectives, plans and programmes, identifying impediments to performance and proposed solutions for avoiding them;
4. exercising the other functions specified by the Center's regulations; and
5. taking all measures necessary to give effect to all the tasks and functions of the Center set out in Article 21 of this Law.

The Chief Executive Officer is assisted in exercising these functions by a sufficient number of experts, technical personnel and administrative personnel, in accordance with the organisational structure of the Center.

Article 24

Members of the Center's Board of Directors and employees of the Center must not divulge any documents, records or data that relate to cases monitored or examined by the Center, or that are submitted or circulated during the examination of those cases or the making of decisions concerning them. This obligation continues after their relationship with the Center ends.

In all circumstances, the information, documents, records and data referred to in this Article must not be disclosed except to investigative authorities and judicial authorities and bodies.

Article 25

The Center may, in coordination with the competent authorities, cooperate with its counterparts in foreign countries under international, regional or bilateral cooperation agreements, under ratified cooperation protocols, or through the application of the principle of reciprocity, for the purposes of protecting Personal Data and verifying the extent to which Controllers and Processors outside the Republic comply with the provisions of the law.

The Center must take steps to exchange data and information in a manner that ensures the protection of Personal Data and prevents their violation, and that assists in investigating related violations and offences and tracking their perpetrators.

Chapter Ten
Licences, Permits and Accreditations

First: Types of Licences, Permits and Accreditations

Article 26

The Center issues Licences, Permits and Accreditations as follows:

1. it classifies Licences, Permits and Accreditations, determines their types and sets the conditions for granting each type, in accordance with the Executive Regulations of this Law;
2. it issues a Licence or Permit to a Controller or Processor to carry out operations for keeping data, dealing with them and Processing them in accordance with this Law;
3. it issues Licences or Permits for direct Electronic Marketing;
4. it issues Licences or Permits for Processing operations carried out by associations, unions or clubs in relation to the Personal Data of their members and within the scope of their activities;
5. it issues Licences or Permits for visual-surveillance methods in public places;
6. it issues Licences or Permits for controlling and Processing Sensitive Personal Data;
7. it issues Permits and Accreditations to entities and individuals, enabling them to provide consultancy services on Personal Data protection procedures and related compliance procedures; and
8. it issues Licences and Permits for the transfer of Personal Data across borders.

The Executive Regulations of this Law must specify the types, categories and levels of these Licences, Permits and Accreditations, the procedures and conditions for their issue and renewal, and the forms to be used. The fee for a Licence must not exceed two million Egyptian pounds and the fee for a Permit or Accreditation must not exceed five hundred thousand Egyptian pounds.

Second: Procedures for Issuing Licences, Permits and Accreditations

Article 27

Applications for Licences, Permits and Accreditations must be made on the forms prescribed by the Center and accompanied by all the documents and information specified by it, together with evidence of the applicant's financial capacity and ability to satisfy the prescribed technical requirements and implement the prescribed technical standards. An application must be determined within a period not exceeding ninety days from the date on which all the required documents and information have been provided; otherwise, the application is deemed refused.

The Center may request additional data, records or documents for the purpose of determining the application. It may also require additional safeguards for the protection of Personal Data if the protection described in the documents submitted to it proves insufficient.

A Controller or Processor may obtain more than one Licence or Permit, depending on the type of Personal Data handled.

Third: Amendment of the Conditions of Licences and Permits

Article 28

The Center may, for reasons of public interest, amend the conditions of a Licence or Permit after it has been issued if:

1. the amendment gives effect to relevant international or regional agreements or national laws;
2. the licensee requests the amendment;
3. a Controller or Processor merges with others, whether within or outside the Arab Republic of Egypt; or
4. the amendment is necessary to achieve the purposes of this Law.

Fourth: Cancellation of Licences, Permits and Accreditations

Article 29

The Center may cancel a Licence, Permit or Accreditation after it has been issued in any of the following cases:

1. breach of the conditions of the Licence, Permit or Accreditation;
2. failure to pay the renewal fees for the Licence, Permit or Accreditation;
3. repeated failure to comply with decisions of the Center;
4. assignment of the Licence, Permit or Accreditation to a third party without the approval of the Center; or
5. a judgment declaring the Controller or Processor bankrupt.

Fifth: Administrative Sanctions

Article 30

Without prejudice to civil and criminal liability, where any provision of this Law is contravened, the Chief Executive Officer of the Center must warn the person in breach to cease the contravention and remove its causes or effects within a period specified by the Chief Executive Officer. If that period expires without compliance with the warning, the Center's Board of Directors may, by a reasoned decision:

1. issue a warning that the Licence, Permit or Accreditation may be suspended, in whole or in part, for a specified period;
2. suspend the Licence, Permit or Accreditation, in whole or in part;
3. withdraw or cancel the Licence, Permit or Accreditation, in whole or in part;
4. publish, at the expense of the person in breach, a statement of the contraventions established to have occurred, in one or more widely circulated media outlets; or
5. place the Controller or Processor under the technical supervision of the Center, at the expense of the Controller or Processor concerned, to secure the protection of Personal Data.

Chapter Eleven
Budget and Financial Resources of the Center

Article 31

The Center has a separate budget prepared in accordance with the model used for the budgets of economic authorities and the rules specified by the Center's regulations. The budget follows the rules of the Unified Accounting System but is not subject to governmental rules and systems.

The Center's financial year coincides with the State's financial year. The Center has a special account with the Central Bank into which its resources are deposited. With the approval of the Minister of Finance, it may also open an account in its name with a commercial bank.

Any surplus in the Center's budget is carried forward from one financial year to the next. Expenditure from its resources must be made in accordance with its financial regulations and in the fields determined by its Board of Directors.

The Center's resources consist of:

1. amounts allocated to it from the budget of the Information Technology Industry Development Agency;
2. amounts allocated to it from the Public Treasury, totalling not less than one-third of the proceeds of fines imposed by a court under this Law;
3. charges for services provided by the Center;
4. fees and charges for Licences, Permits and Accreditations issued by the Center, and amounts received from settlements accepted by it;
5. returns on the investment of the Center's funds; and
6. grants, donations and gifts accepted by the Board of Directors.

Chapter Twelve
Requests and Complaints

First: Requests

Article 32

The Data Subject or any person with standing may submit a request to any Holder, Controller or Processor concerning the exercise of the rights provided for in this Law. The person to whom the request is submitted must respond within six working days from the date on which it was submitted.

Second: Complaints

Article 33

Without prejudice to the right to have recourse to the courts, the Data Subject and any person with standing and a direct interest have the right to lodge a complaint in any of the following cases:

1. violation or impairment of the right to the protection of Personal Data;

2. refusal to enable the Data Subject to exercise their rights; or

3. a decision issued by the Data Protection Officer of a Processor or Controller concerning a request submitted to that officer.

The complaint must be submitted to the Center, which may take any investigative measures necessary. The Center must issue its decision within thirty working days from the date on which the complaint was submitted and notify the complainant and the person against whom the complaint was made of that decision.

The person against whom the complaint was made must implement the Center's decision within seven working days from the date on which that person was notified of it and inform the Center of the steps taken to implement it.

Chapter Thirteen
Judicial Enforcement Officer Status

Article 34

The employees of the Center designated by a decision of the Minister of Justice, issued on the proposal of the Competent Minister, are vested with the status of judicial enforcement officers for the purpose of establishing the commission of offences in contravention of this Law.

Chapter Fourteen
Offences and Penalties

Article 35

Without prejudice to any more severe penalty prescribed by any other law, and without prejudice to the right of the person harmed by the offence to compensation, the offences provided for in the following Articles are punishable by the penalties prescribed for them.

Article 36

A Holder, Controller or Processor who collects, Processes, divulges, makes available or circulates electronically Processed Personal Data, by any means, in circumstances other than those authorised by law or without the Data Subject's consent is punishable by a fine of not less than one hundred thousand Egyptian pounds and not more than one million Egyptian pounds.

If that conduct is committed in return for a material or non-material benefit, or with the intention of exposing the Data Subject to danger or harm, the penalty is imprisonment for a term of not less than six months and a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds, or either of those penalties.

Article 37

A Holder, Controller or Processor who, without legal justification, refuses to enable the Data Subject to exercise the rights set out in Article 2 of this Law is punishable by a fine of not less than one hundred thousand Egyptian pounds and not more than one million Egyptian pounds. A person who collects Personal Data when the conditions set out in Article 3 of this Law are not met is punishable by a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds.

Article 38

A Controller or Processor who fails to comply with the duties set out in Articles 4, 5 and 7 of this Law is punishable by a fine of not less than three hundred thousand Egyptian pounds and not more than three million Egyptian pounds.

Article 39

A legal representative of a legal person who fails to comply with any duty imposed on that representative under Article 8 of this Law is punishable by a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds.

Article 40

A Data Protection Officer who fails to comply with the requirements of that officer's role set out in Article 9 of this Law is punishable by a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds.

If the offence occurs as a result of negligence by the Data Protection Officer, that officer is punishable by a fine of not less than fifty thousand Egyptian pounds and not more than five hundred thousand Egyptian pounds.

Article 41

A Holder, Controller or Processor who collects, makes available, circulates, Processes, divulges, stores, transfers or keeps Sensitive Personal Data without the Data Subject's consent or in circumstances not authorised by law is punishable by imprisonment for a term of not less than three months and a fine of not less than five hundred thousand Egyptian pounds and not more than five million Egyptian pounds, or by either of those penalties.

Article 42

A person who contravenes the provisions on Cross-Border Movement of Personal Data set out in Articles 14, 15 and 16 of this Law is punishable by imprisonment for a term of not less than three months and a fine of not less than five hundred thousand Egyptian pounds and not more than five million Egyptian pounds, or by either of those penalties.

Article 43

A person who contravenes the Electronic Marketing provisions set out in Articles 17 and 18 of this Law is punishable by a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds.

Article 44

A member of the Board of Directors or an employee of the Center who contravenes the obligations set out in Article 24 of this Law is punishable by a fine of not less than three hundred thousand Egyptian pounds and not more than three million Egyptian pounds.

Article 45

A person who contravenes the provisions on Licences, Permits or Accreditations set out in this Law is punishable by a fine of not less than five hundred thousand Egyptian pounds and not more than five million Egyptian pounds.

Article 46

A person who prevents an employee of the Center who is vested with the status of a judicial enforcement officer from performing that employee's duties is punishable by imprisonment for a term of not less than six months and a fine of not less than two hundred thousand Egyptian pounds and not more than two million Egyptian pounds, or by either of those penalties.

Article 47

The person responsible for the actual management of a legal person that has contravened this Law is punishable by the same penalties prescribed for the acts committed in contravention of this Law if it is proved that the person knew of those acts and that a breach by that person of the duties imposed on them in that managerial capacity contributed to the commission of the offence.

The legal person is jointly and severally liable for payment of any compensation awarded if the contravention was committed by one of its employees in its name and for its benefit.

Article 48

In all cases, in addition to the penalties provided for in this Law, the court must order publication of the judgment of conviction in two widely circulated newspapers and on open electronic information networks, at the expense of the person convicted.

In the event of recidivism, both the minimum and maximum limits of the penalties set out in this Chapter are doubled.

An attempt to commit any of the offences provided for in this Law is punishable by half the penalty prescribed for that offence.

Reconciliation and Settlement

Article 49

At any stage of the criminal proceedings and before the judgment becomes final, the accused may, with the Center's approval, establish before the Public Prosecution or the competent court, as the case may be, that reconciliation has been reached with the victim, the victim's specially authorised agent or the victim's universal successor, in respect of the misdemeanours provided for in Articles 36, 37, 38, 39, 40, 41 and 43 of this Law.

Settlement may be reached with the Center, at any stage of the proceedings, in respect of the misdemeanours provided for in Articles 42, 44 and 45 of this Law.

In all cases, an accused who wishes to settle before criminal proceedings are instituted must pay an amount equal to half the minimum fine prescribed for the offence.

An accused who wishes to settle after criminal proceedings have been instituted and before the judgment becomes final must pay half the maximum fine prescribed for the offence or the amount of the fine imposed, whichever is greater.

Payment must be made to the treasury of the competent court, the Public Prosecution or the Center, as the case may be.

Settlement terminates the criminal proceedings without affecting the rights of any person harmed by the offence.