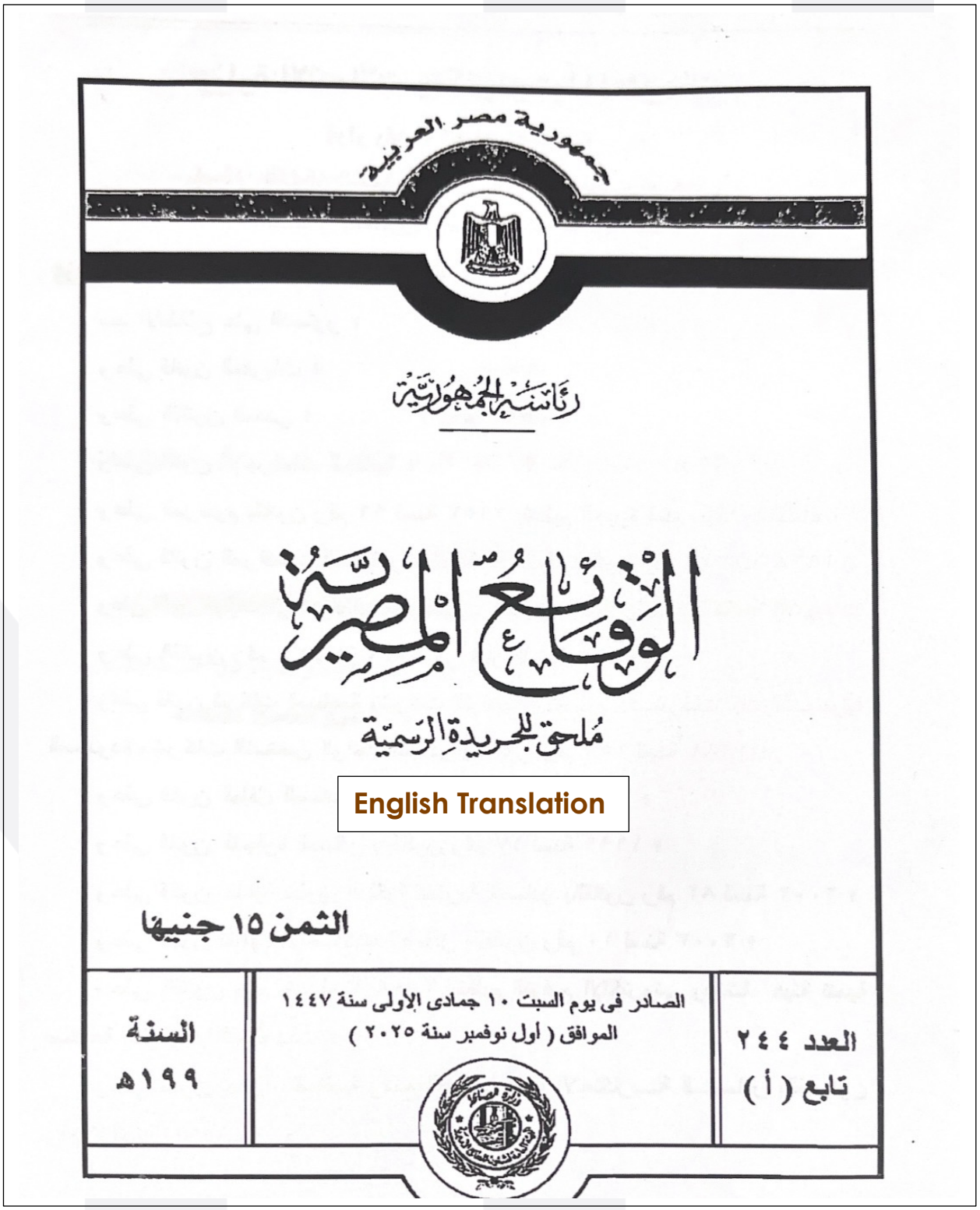

جمهورية مصر العربية

رئاسة الجمهورية

الوقائع المصرية

ملحق للجريدة الرسمية

English Translation

الثمن ١٥ جنيها

السنة	الصادر فى يوم السبت ١٠ جمادى الأولى سنة ١٤٤٧ الموافق (أول نوفمبر سنة ٢٠٢٥)	العدد ٢٤٤ تابع (أ)
١٩٩ ه		

Ministry of Communications and Information Technology

Decision No. 816 of 2025

Issuing the Executive Regulations of the Personal Data Protection Law

Issued by Law No. 151 of 2020

Minister of Communications and Information Technology

Having reviewed the Constitution;

and the Penal Code;

and the Civil Code;

and the Code of Criminal Procedure;

and Decree-Law No. 96 of 1952 Regulating Expert Testimony before the Judiciary;

and the Code of Civil and Commercial Procedure issued by Law No. 13 of 1968;

and the Law of Evidence in Civil and Commercial Matters issued by Law No. 25 of 1968;

and Law No. 34 of 1976 Concerning the Commercial Register;

and the Law on Joint Stock Companies, Limited Partnerships by Shares, Limited Liability Companies, Limited Liability Companies, and Single-Person Companies issued by Law No. 159 of 1981;

and the Child Law issued by Law No. 12 of 1996;

and on the Commercial Code issued by Law No. 17 of 1999;

and on the Intellectual Property Rights Protection Law issued by Law No. 82 of 2002;

and on the Telecommunications Regulation Law issued by Law No. 10 of 2003;

and on Law No. 15 of 2004 Regulating Electronic Signatures and Establishing the Information Technology Industry Development Authority;

and on the Competition Protection and Anti-Monopoly Practices Law issued by Law No. 3 of 2005;

and on the Law Regulating Land Passenger Transport Services Using Information Technology issued by Law No. 87 of 2018;

and on Law No. 175 of 2018 on Combating Information Technology Crimes;

and on the Consumer Protection Law issued by Law No. 181 of 2018;

and on the Central Bank and Banking System Law issued by Law No. 194 of 2020;

And based on the opinion of the State Council;

It was decided:

(Article 1)

The provisions of the Executive Regulations accompanying this decision regarding the aforementioned Personal Data Protection Law shall be implemented.

(Article 2)

This decision shall be published in the Egyptian Gazette and shall come into effect on the day following its publication.

Minister of Communications and Information Technology

Dr. Amr Samih Talaat

Table of Contents

Executive Regulations

of the Personal Data Protection Law

Article 1

For the purposes of these Regulations, the definitions contained in the aforementioned Personal Data Protection Law shall have the same meaning intended therein. For the purposes of these Regulations, the "**Law**" shall mean: the Egyptian Personal Data Protection Law issued by Law No. 151 of 2020.

Article 2

(The collection, processing, storage, and securing of personal data shall be in accordance with the following controls, standards, procedures, and policies)

The collection, processing, storage, and securing of personal data shall be in accordance with the following controls, standards, procedures, and policies:

- **First - Controls and Standards:**
  1. The entity collecting personal data must hold a license or permit as a controller or processor, without prejudice to the obligations stipulated by the competent authorities for conducting the activity
  2. Personal data shall only be collected after obtaining the consent of the data subject and clearly informing them of the purpose of its collection. A natural person's provision of their personal data in the course of receiving legitimate services or transactions shall be considered consent to the data being obtained and processed for that purpose. This data may not be used for any other purpose without prior consent.
  3. Obtaining the Center's approval of the mechanisms used in collecting personal data, and the mechanism for obtaining the consent of the data subject or their guardian in the case of children's data
  4. Determining the time period required to retain collected personal data according to the purpose of its collection
  5. The obligation of those responsible for collecting personal data to maintain its confidentiality and not to use, circulate, or disclose it in any way except for the reasons stipulated by law and in accordance with the license or permit issued in this regard.
- **Second - Procedures and Policies:**

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

1. Informing the data subject of their rights in accordance with Article (2) of the Law
2. Taking the security procedures and programs issued by the Center and that must be followed regarding the security of personal data, including the devices and media used.
3. Relying in work policies on preparing a secure electronic record that includes recording the following:
    - The consent of the data subject, the date of issuance of this consent, and the format in which it was issued
    - A description of the categories of personal data that are collected and the scope of their use
    - The time period required to retain each category of personal data separately, and its relation to the purpose thereof
    - The organizational and technical procedures followed regarding data security that enable the Center to conduct periodic inspections and verify the licensee's or permit holder's compliance with it

Article 3

(Policies, procedures, controls, and technical standards for the obligations of the personal data controller)

The obligations of the personal data controller shall be in accordance with the following technical controls, standards, procedures, and policies:

- **First - Technical Controls and Standards:**
    1. Obtaining a license or permit from the Center in accordance with the categories, conditions, and procedures specified in these regulations, without prejudice to the obligations stipulated by the competent authorities for conducting the activity
    2. Compliance with the licensed or authorized purpose for the use of personal data collected and processed, as stipulated in the license or permit issued to the controller by the Center.
    3. Verification that the collected personal data is accurate by reviewing its source, whether from its employees or the data subject themselves, and the extent to

which such data is consistent with the purpose of its collection and processing, in accordance with the conditions stipulated in the license or permit issued to the controller by the Center.

4. Deletion of personal data immediately upon completion of the purpose for which it was retained, and notification of the data subject of this deletion. Such data may not remain in a form that allows the identification of the data subject if retained for any legitimate reason after the purpose for which it was retained has ended.
5. Establishment of a mechanism approved by the Center that allows the data subject to submit a request to access and review their personal data, withdraw prior consent to its retention, correct or amend their data, limit it for processing within a specific scope, or object to any processing of it
6. A controller located outside the Arab Republic of Egypt, and without a branch or representative office within the country, is obligated to appoint a representative within the country through a branch of the company or an office acting on its behalf or representing it, as the case may be. This representative shall be accredited by the Center as the controller's representative for the duration of the license or permit. If the controller is a natural person, they are obligated to appoint an agent within the Arab Republic of Egypt.
7. Enabling the Center's inspectors, in their capacity as judicial officers, to access electronic records and verify the application of standard criteria and technical procedures related to data security and protection, and any executive decisions issued by the Center in this regard.
8. The controller is obligated to provide the volume and type of personal data that the law regulating its activity permits it to obtain. The rules and regulations stipulated in the law shall apply to any additional personal data upon its request, including rules for retention, security, and transfer, in the absence of such rules and regulations in the law regulating its activity
9. Taking the necessary procedures and measures to obligate those responsible for collecting personal data to maintain the confidentiality of that data and not to use, circulate, or disclose it in any way except for legally prescribed reasons.

- **Second - Procedures and Policies:**
  1. Conducting periodic testing and evaluation processes to ensure the accuracy and integrity of the collected personal data, in accordance with the periodic evaluation and examination mechanisms issued by the Center.
  2. Taking the necessary procedures and measures to ensure that the data of the person concerned is in an unreadable form, and that this data does not remain in a form that allows the identification of the data subject, in the event that the controller retains it based on legal reasons or national security considerations, provided that this data is deleted upon the termination of the legal reason or purpose for which it was retained.
  3. Taking the necessary technical procedures to maintain the confidentiality of the data and prevent its breach.
  4. Taking the technical and organizational procedures that ensure its ability to recover the data, access to it in a timely manner, and its confiscation in the event of any physical or technical incident.
  5. Without prejudice to the obligation to prepare electronic records referred to in Article (2) of these Regulations, the entity controlling its work policy shall be obligated to prepare secure electronic records, which shall include the following:
     - Requests from the data subject regarding the addition or modification of their personal data, provided that this includes recording the data to be modified and indicating whether the modification has been completed or not, and the reason for this.
     - Requests from the data subject regarding the deletion of their data, and retraction of their previous consent, indicating whether the deletion process has been completed or not, and the mechanism for notifying the data subject of this.
     - Personal data that is withheld for legal reasons or for national security considerations, in a manner that allows the center's inspectors to verify the application of standard criteria and technical procedures for securing and protecting such data, without allowing others to identify the data subject

Article 4

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

(Policies, Procedures, Controls, Conditions, Instructions, and Standards for the Obligations of the Personal Data Processor)

The processing of personal data shall be in accordance with the following controls, standards, procedures, and policies:

- **First – Controls and Standards:**
    1. Obtaining a license or permit from the Center in accordance with the categories, conditions, and procedures specified in these regulations, without prejudice to the obligations stipulated by the competent authorities for conducting the activity.
    2. Preparing a mechanism to be approved by the Center that determines the volume of personal data and the purpose of processing, and that allows for recording the consent of the data subject to this and that it indicates notification to the controller, the data subject, and any other interested party of the period required for processing
    3. Data handlers employed by the processor are obligated to maintain the confidentiality of personal data and not to use, share, or disclose it in any way except for reasons stipulated by law.
    4. Enabling the Center's inspectors, in their capacity as judicial officers, to review electronic records and verify the application of standard criteria and technical procedures for data security and protection, as well as any executive decisions issued by the Center in this regard, and ensuring that the processing purposes conform to the nature of the activity licensed by the Center.
    5. A processor located outside the Arab Republic of Egypt, and without a branch or representative office within the country, is obligated to appoint a representative within the country through a branch of the company or an office acting on its behalf or representing it, as the case may be. This representative shall be accredited by the Center as the processor's representative for the duration of the license or permit. If the processor is a natural person, they are obligated to appoint an agent within the Arab Republic of Egypt

6. Prohibition of processing any personal data for a purpose other than that of the controller or its activity, except for statistical or educational purposes and for non-profit purposes, and under the following conditions:
   (a) Obligation to obtain the consent of the data subject.
   (b) That the subject of the study be relevant to the personal data being processed.
   (c) If personal data is handled in any form, it must be encoded so that the data subject cannot be identified.
7. Obligation of the processor to handle personal data, when processing and using it for training artificial intelligence and emerging and innovative technologies, in accordance with locally, regionally and internationally recognized principles, in a manner that ensures the use of these technologies does not cause any harm to the data subject
8. The processor is obligated to obtain the volume and type of personal data that the law regulating its activity allows it to access, and to apply the rules and controls stipulated in the law to any additional personal data upon its request, including rules for retention, security, and transfer, in the absence of such rules and controls in the law regulating its activity

- **Second - Procedures and Policies:**

1. Taking the necessary security procedures and measures to secure and protect personal data during its processing, including the devices and media used, and storing personal data in an unreadable form to ensure its confidentiality and the inability to link it to the data subject by unauthorized persons.
2. Taking the technical and organizational procedures that ensure its ability to recover and access personal data in a timely manner, and to contain it in the event of any physical or technical incident
3. Relying in work policies on the preparation of a secure electronic record, which includes the following:

- A record and description of the processing operations it performs, the categories of personal data it uses, and the scope of their use, provided that

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

the record includes the processor's data, a copy of the processing contract concluded with the controller, and the data protection officer's data pertaining to the controller, the data of the controller's legal representative, processing standards, and in the case of cross-border data transfer, a clarification of the countries to which the data is transferred, the systems for securing it and the data route, and a general description of the technical standards used to protect the data.

- The time periods required to process each category of personal data separately.
- The organizational and technical procedures followed regarding data security, processing and storage operations, enabling the center to conduct periodic inspections and verify the processor's compliance with them.
- Recording the date and time of the data erasure process after completion of processing or proof of its delivery to the controller in accordance with the legally prescribed circumstances.

Article 5

(Obligations of the controller and processor in cases of breach or violation of personal data)

The controller and processor, as applicable, are obligated to notify the Center, through the electronic portal or the hotline established for this purpose, within seventy-two hours of becoming aware of the breach or violation, in the event of a breach or violation. This notification must be recorded in a secure electronic log prepared for this purpose, and must include the following:

1. The hour and date of becoming aware of the breach or violation and the time of reporting it.
2. A description of the nature of the breach or violation and the time of its occurrence, enabling the Center to verify an approximate estimate of the number of compromised data.
3. The potential effects of the breach or violation and the extent of the expected damage.

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

4. The immediate measures and corrective actions taken in response to this breach or violation.
5. The contact information of their data protection officer.
6. Any additional documents, data, or information requested by the Center

If the breach or violation is related to national security considerations or the entities responsible for them, the report must be submitted to the center immediately and must include, in addition to the conditions in the information referred to in the previous paragraph is as follows:

(a) The connection of the breach or violation to considerations of protecting national security.

(b) The volume of data affected by the breach or violation and an estimate of the resulting damage about that

In all cases, the controller and the processor, as applicable, are obligated to notify the data subject within three working days of the date the center is notified of the breach or violation, and of the safeguards taken, by the agreed-upon means (text message, email, telephone call), as specified upon consent to collect his data.

Article 6

(Center's obligations in cases of breach or violation of personal data)

The center must provide methods and means of communication for reporting breaches or violations of personal data, taking into account the adoption of a specific communication method for receiving reports related to national security considerations.

The center is also committed to coordinating with national security agencies to determine the mechanisms for notifying them in the event of receiving reports related to a breach or violation of personal data.

The center works to train and raise awareness among personal data protection officers on a regular basis regarding standards for classifying the nature of a breach or violation.

Article 7

(Conditions for Registering Personal Data Protection Officers)

The following conditions are required for registering personal data protection officers:

1. The applicant must possess academic qualifications or professional certificates, along with practical experience in relevant fields, according to the standards adopted by the Board of Directors of the Center for the purpose of protecting personal data.
2. Passing the tests approved by the Center according to the nature and size of the personal data activity for which registration is requested.
3. Not having been previously convicted of any crimes involving moral turpitude or dishonesty.

Article 8

(Registration Documents in the Register of Personal Data Protection Officers)

The application for registration in the Register of Personal Data Protection Officers shall be submitted, accompanied by the following documents:

1. A copy of the applicant's personal identification card (National ID for Egyptians - Passport for foreigners).
2. A recent personal photograph.
3. The academic qualifications obtained.
4. The duration of practical experience in relevant fields.
5. Criminal record certificate for Egyptians, and for foreigners, duly authenticated by the relevant authorities.
6. Proof of passing the tests prescribed by the center for registration.
7. The Personal Data Protection Officer's code, if previously registered in the Personal Data Protection Officers' register at the center, controller, or another processor, or if registered as a natural person and wishes to register with a controller or processor.

The Center shall study the application and notify the applicant of the acceptance or rejection of their registration within thirty working days from the date of application. The Center may request the submission of any documents necessary for deciding on the application within a period it specifies, provided that the applicant is notified of the

acceptance or rejection of their registration within fifteen days from the date of submission of the documents.

The legal representative of any entity shall take the necessary measures to register personal data protection officers to enable them to perform their duties in accordance with the provisions of the law.

Article 9

(Registration of Personal Data Protection Officers)

An electronic register shall be established at the Center dedicated to registering Personal Data Protection Officers. Each officer shall have an identification number called the (Personal Data Protection Officer Code,) which shall include the nature and volume of data they are authorized to handle, based on their test results. All their personal data may be accessed through this code.

Registration shall be done through the electronic portal on the register dedicated to registering the Personal Data Protection Officer at the Center, via the designated links, through any of the following:

1. An application submitted by the legal representative of the controller or processor to register an employee in the register of Personal Data Protection Officers, including proof of meeting the registration requirements and the volume and nature of the data they are authorized to handle.
2. An application submitted by a natural person, including proof of meeting the registration requirements and the volume and nature of the data they are authorized to handle.

The Personal Data Protection Officer Code shall be determined based on their meeting the registration requirements.

Article 10

(Termination of the contractual relationship or replacement of Personal Data Protection Officers - DPOs)

The legal representative of any controller or processor, if wishing to terminate the relationship with the data protection officer, must notify the Center at least fifteen days prior to the termination of this relationship, provided that they have submitted a request to register or appoint another data protection officer (other than the current one), whether from its organizational structure or contracted with, in accordance with the nature and volume of data previously handled during that period, specifying the code of the alternative data protection officer, and the period stipulated for performing these tasks if his appointment is temporary, through the electronic portal of the Center or any other means of communication approved by the Center.

The Center may suspend the registered personal data protection officer and request his replacement, in the event of his violation of any of the registration conditions, and the legal representative in this case must register a temporary alternative personal data protection officer from those registered with the Center, whether from its organizational structure or contracted with for the same volume and nature of data handled, until a permanent officer is appointed within a period to be determined by the Center

The legal representative must also provide the Center with the means of contacting the alternate data protection officer.

Article 11

(Limits of Jurisdiction Personal Data Protection Officer)

A personal data protection officer registered with the Center may perform their duties in one or more functional structures, provided the following two conditions are met:

1. The entities for which the personal data protection officer is registered agree to perform their duties for other entities or legal persons, without this leading to a conflict of interest, and provided that this is within the limits of the volume and nature of the data the personal data protection officer is authorized to handle.
2. The Center approves the registration of a personal data protection officer for more than one entity, according to the nature and volume of the activity of those entities, and after ensuring that there is no conflict or breach of their duties as a result.

One personal data protection officer may be registered for entities that are structurally or organizationally linked and whose activity is complementary through data exchange, provided that the Center is notified of this.

Article 12

(Obligations of the Personal Data Protection Officer)

The Data Protection Officer is obligated to:

1. Monitor the application of the security policies issued by the Center related to securing the processing, storage, and handling of data, and submit an annual report to the Center on the state of privacy protection at the controller or processor, or upon request.
2. The alternate Data Protection Officer shall submit a report to the Center, within 15 days of assuming their duties, on the state of privacy protection, in the event of a change in the Data Protection Officer according to the cases stipulated in Article (10) of these Regulations.
3. Monitor the process of receiving reports and complaints related to data subjects regarding requests to delete, modify, or add their personal data and ensure their implementation.
4. Ensure that their duties do not conflict with any other assignments that could harm the protection of personal data
5. Establishing a separate system when the Personal Data Protection Officer is assigned to a group of bodies, institutions, or companies, to assist him in performing his duties and responsibilities, and to enable the Center to review it.

Article 13

(Digital Evidence)

Digital evidence derived from personal data shall have the same evidentiary weight as evidence derived from written data and information, if it meets the following standards and technical conditions:

1. The process of collecting or extracting the digital evidence related to personal data must be carried out using technologies that ensure that the personal data and related information are not altered, updated, erased, or distorted.
2. The digital evidence must be relevant to the incident and within the scope of the subject matter, proving or disproving it according to the scope of the decision of the investigating authority or the competent court.
3. The evidence shall be collected, extracted, and preserved by judicial officers authorized to handle this type of evidence or by specialized experts from the investigation or trial authorities. The seizure reports or technical reports shall specify the type and specifications of the programs, tools, and devices used and ensure the preservation of the original without tampering.
4. Digital evidence shall be documented in a procedural report by the competent authority before examination and analysis by printing copies of the stored files or photographing them by any visual or digital means and having them approved by those responsible for collecting, extracting, or analyzing the digital evidence. Each copy shall include the date and time of printing and photographing, the name of the person performing the task, details of the devices, equipment, and tools used, and the data and information pertaining to the content of the seized evidence.

Article 14

(Standards and Controls for Handling Sensitive Personal Data)

The controller or processor, as the case may be, whether a natural or legal person, is obligated to comply with the following controls and standards when collecting, transferring, storing, preserving, processing, or making available sensitive personal data:

1. Obtaining a license or permit from the Center in accordance with the nature of its activity and the categories of licenses and permits specified in these regulations.
2. Obtaining explicit written consent (in paper or electronic form) from the data subject or their guardian in the case of children's data, except in cases permitted by law.
3. This data must be essential and necessary for the purpose specific to the nature of the controller's or processor's work, and its use must not cause harm to the data subject.

4. Compliance with the security standards established by the Center regarding the handling of sensitive personal data.
5. In the event of a child's participation in a game, competition, or any other activity, they must not receive more than what is necessary for participation, and this data must not be used in the classification, tracking, or behavioral monitoring of children.
6. Any other standards adopted by the Center's Board of Directors that aim to protect sensitive personal data
7. Maintaining secure electronic records in accordance with the Center's requirements regarding the following:

   (a) Recording the consents of the data subject or the child's guardian when dealing with such data in any of the aforementioned ways.

   (b) Recording requests to delete, erase, modify, or stop processing sensitive personal data submitted by the data subject or the child's guardian, and proof of their activation.

Article 15

(Standards and controls specific to dealing with children's data)

Those who possess, control, or process the data of children under 15 years of age must obtain, before collecting their data, explicit written consent (paper or electronic) from the guardian to collect and process their data for the purpose of providing a service or for any other purpose. The consent must include the timeframe for its collection and processing, without prejudice to the guardian's right to withdraw or amend their consent. The Center shall approve the mechanisms and formats through which such consents are issued.

In the case of children aged 15 to 18 years, the child or their guardian, as the case may be, are obligated to provide the latter's consent to the collection and processing of the child's data. The Center shall determine the mechanisms for this for the guardian, ensuring compliance with the legal requirements stipulated in this regard.

Article 16

(Policies, standards, controls, and rules necessary for the transfer, storage, sharing, processing, making available, or protection of personal data across borders)

The transfer, storage, sharing, processing, or making available of personal data across borders shall be in accordance with the following controls, rules, policies, and standards:

- First - Controls and rules:

1. The controller or processor, as the case may be, shall, when transferring personal data that has been collected or prepared for processing to a foreign country for processing, storage, or sharing, have obtained a license or permit to do so from the Center in accordance with its assessment of the adequacy of the level of protection in that country
2. The controller or processor, as applicable, is obligated to obtain the consent of the data subject when transferring personal data collected or prepared for processing to a foreign country for processing, storage, or sharing.
3. The controller or processor is obligated to take all actions and measures that ensure the use of technologies that guarantee an adequate level of protection for personal data during its transfer, handling, sharing, or storage, in accordance with the license or permit issued to it by the Center and in a manner commensurate with the volume and nature of the data that it is licensed or authorized to transfer, share, handle, store, or process across borders.
4. The controller or processor, as applicable, is obligated to transfer personal data that has been collected or prepared for processing to the foreign country or countries as stated in the license or permit issued by the Center in this regard and is obligated to update the license or permit if other countries are added during the license or permit period

- **Second - Policies and Standards:**

The Center shall determine in the policies it adopts the countries that guarantee a sufficient level of protection for personal data in accordance with the provisions of the law, provided that this does not prejudice the establishment of a mechanism for periodic review, in accordance with the following standards:

1. The existence of legislation or regulations related to the protection of personal data and their consistency with the provisions of the law.

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

2. The availability of technical and security rules and measures that achieve the protection of personal data
3. The availability of legal rules for compensation for damages that may befall the data subject in the event of misuse of his personal data.

In light of the availability of the aforementioned standards, the Center may approve the issuance of a license or permit to the controller or processor, as the case may be, to transfer, store, or share such data to any other foreign countries that meet the same standards.

Article 17

(The requirements, procedures, precautions, standards, and rules necessary for making personal data available to another controller or processor outside the Arab Republic of Egypt)

The controller or processor may, as the case may be, make personal data available to another controller or processor outside the Arab Republic of Egypt with a license from the Center, in accordance with the following conditions, restrictions, and standards:

1. The activities of the group of projects or companies must be of a common or complementary nature of work, in a way that achieves a legitimate interest for both parties or for the data subject.
2. Precautions must be taken to achieve a level of legal and technical protection for personal data held by the controller or processor located abroad that is no less than that applied in the Arab Republic of Egypt.

Article 18

(Rules, Conditions and Regulations Regarding Direct Electronic Marketing)

The sender, whether controller or processor, of any electronic communication for the purpose of direct marketing, shall comply with the following rules, conditions and controls:

- **First - Rules and Conditions:**

1. To have a license from the center to conduct direct electronic marketing activities
2. He must have obtained explicit consent from the data subject to receive the marketing communication

3. The controller, processor, or marketing intermediary must erase personal data, In the following two cases:

   (a) Withdrawal of consent by the data subject to the use of his data for the purpose of Electronic marketing.

   (b) Expiration of the data retention period or cessation of the marketing purpose, whichever is closer.

- **Second - Controls:**

1. Personal data collected for electronic marketing activities shall not be used for any other purpose, exchanged, or processed for any other purpose except with the explicit consent of the person concerned.
2. The initial contact must include the caller's identity and specify the marketing purpose, enabling the person concerned to exercise their right to refuse the contact or withdraw their prior consent, through any of the communication methods approved by the center for this purpose, whether by sending personal messages via social media, text messages, email, telephone calls, or any other technological means.
3. The sender, if acting as a marketing intermediary, must ensure that the controller or processor obtains the consent of the data subject to accept the marketing communication for its declared purposes. The sender is also obligated to retain the source of the data obtained from the data subject, including their consent to its use. Otherwise, the sender must immediately cease using that data in the field of electronic marketing.
4. Maintaining electronic records, made available to the Center upon request, including the following:

   (a) How and when the data subject's consent to accept electronic marketing was obtained, and its specific purpose.

   (b) Requests to erase or amend that consent and the actions taken in response.

   (c) Mechanisms for securing and preserving personal data in accordance with the procedures adopted by the Center.

In all cases, the Center shall allocate a means of communication to receive citizens' complaints related to direct electronic marketing, whether through its website or short telephone numbers.

Article 19

(Classification and categories of controller and/or processor license for personal data and sensitive personal data)

The Center issues a Controller/Processor Consortium License for legal entities, according to the following tables:

Number of Records for Individuals' Personal Data	**Annual Value of License Fees for Controller/Processor**
From 1 to 100,000	Exempt from License Fees
From 101,000 to 200,000	200 EGP (Egyptian Pound)
From 201,000 to 300,000	300 EGP (Egyptian Pound)
From 301,000 to 400,000	400 EGP (Egyptian Pound)
From 401,000 to 500,000	500 EGP (Egyptian Pound)
From 501,000 to 600,000	600 EGP (Egyptian Pound)
From 601,000 to 700,000	700 EGP (Egyptian Pound)
From 701,000 to 800,000	800 EGP (Egyptian Pound)
From 801,000 to 900,000	900 EGP (Egyptian Pound)
From 901,000 to 1,000,000	1,000 EGP (Egyptian Pound)

The value of One Hundred Thousand personal data records exceeding One Million and up to Two Million records is calculated at Five Thousand Egyptian Pounds, as follows:

Number of Records for Individuals' Personal Data	**Annual Value of License Fees for Controller/Processor**
From 1,001,000 to 1,100,000	5,000 EGP (Egyptian Pound)

From 1,101,000 to 1,200,000	10,000 EGP (Egyptian Pound)
From 1,201,000 to 1,300,000	15,000 EGP (Egyptian Pound)
From 1,301,000 to 1,400,000	20,000 EGP (Egyptian Pound)
From 1,401,000 to 1,500,000	25,000 EGP (Egyptian Pound)
From 1,501,000 to 1,600,000	30,000 EGP (Egyptian Pound)
From 1,601,000 to 1,700,000	35,000 EGP (Egyptian Pound)
From 1,701,000 to 1,800,000	40,000 EGP (Egyptian Pound)
From 1,801,000 to 1,900,000	45,000 EGP (Egyptian Pound)
From 1,901,000 to 2,000,000	50,000 EGP (Egyptian Pound)

The value of One Hundred Thousand personal data records, exceeding Two Million records and up to Three Million, is calculated at Ten Thousand Egyptian Pounds, as follows:

Number of Records for Individuals' Personal Data	**Annual Value of License Fees for Controller/Processor**
From 2,001,000 to 2,100,000	60,000 EGP (Egyptian Pound)
From 2,101,000 to 2,200,000	70,000 EGP (Egyptian Pound)
From 2,200,001 to 2,300,000	80,000 EGP (Egyptian Pound)
From 2,300,001 to 2,400,000	90,000 EGP (Egyptian Pound)
From 2,400,001 to 2,500,000	100,000 EGP (Egyptian Pound)
From 2,500,001 to 2,600,000	110,000 EGP (Egyptian Pound)
From 2,600,001 to 2,700,000	120,000 EGP (Egyptian Pound)
From 2,700,001 to 2,800,000	130,000 EGP (Egyptian Pound)
From 2,801,000 to 2,900,000	140,000 EGP (Egyptian Pound)
From 2,900,001 to 3,000,000	150,000 EGP (Egyptian Pound)

The value of One Hundred Thousand personal data records, exceeding Three Million records and up to Four Million, is calculated at Fifteen Thousand Egyptian Pounds, as follows:

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt

Number of Records for Individuals' Personal Data	Annual Value of License Fees for Controller/Processor
From 3,001,000 to 3,100,000	165,000 EGP (Egyptian Pound)
From 3,101,000 to 3,200,000	180,000 EGP (Egyptian Pound)
From 3,200,001 to 3,300,000	195,000 EGP (Egyptian Pound)
From 3,300,001 to 3,400,000	210,000 EGP (Egyptian Pound)
From 3,400,001 to 3,500,000	225,000 EGP (Egyptian Pound)
From 3,500,001 to 3,600,000	240,000 EGP (Egyptian Pound)
From 3,601,000 to 3,700,000	255,000 EGP (Egyptian Pound)
From 3,700,001 to 3,800,000	270,000 EGP (Egyptian Pound)
From 3,800,001 to 3,900,000	285,000 EGP (Egyptian Pound)
From 3,800,001 to 3,900,000	300,000 EGP (Egyptian Pound)

The value of One Hundred Thousand personal data records, exceeding Four Million records and up to Five Million, is calculated at Twenty Thousand Egyptian Pounds, as follows:

Number of Records for Individuals' Personal Data	Annual Value of License Fees for Controller/Processor
From 4,001,000 to 4,100,000	320,000 EGP (Egyptian Pound)
From 4,101,000 to 4,200,000	340,000 EGP (Egyptian Pound)
From 4,200,001 to 4,300,000	360,000 EGP (Egyptian Pound)
From 4,301,000 to 4,400,000	380,000 EGP (Egyptian Pound)
From 4,401,000 to 4,500,000	400,000 EGP (Egyptian Pound)
From 4,501,000 to 4,600,000	420,000 EGP (Egyptian Pound)
From 4,600,001 to 4,700,000	440,000 EGP (Egyptian Pound)
From 4,700,001 to 4,800,000	460,000 EGP (Egyptian Pound)

From 4,800,001 to 4,900,000	480,000 EGP (Egyptian Pound)
From 4,900,001 to 5,000,000	500,000 EGP (Egyptian Pound)

- The licensing fee for data volumes exceeding five million personal data records shall be the maximum legally prescribed amount of 666,666 thousand annually, totaling 2 million EGP, over three years.
- The fees for controller-only or processor-only licenses for legal entities shall be half the value indicated in the table above, according to the data volume.
- The fees for licensing the processing of personal data of members by associations, syndicates, and clubs, **within the scope of their activities, shall be as follows:**

Entity	**Annual Value of License Fee**
Associations	5,000 EGP (Egyptian Pound)
Syndicates	10,000 EGP (Egyptian Pound)
Clubs (number of members' data records - less than 50,000)	20,000 EGP (Egyptian Pound)
Clubs (number of members' data records - more than 50,000)	50,000 EGP (Egyptian Pound)

Article 20

(Classification and Categories of Permits for Controllers and/or Processors of Personal and Sensitive Personal Data)

The Center shall issue a permit for a controller and/or processor for a specific and temporary purpose for varying periods not exceeding one calendar year. The Center shall determine the continuity of this purpose as a condition for obtaining the permit. The permit authorizes the permit holder to obtain personal data and determine the method, style, and standards for retaining, processing, controlling, or transferring it, in accordance with the

purpose specified in the permit and in a manner that does not conflict with the provisions of the law and these regulations.

The permit fee is determined according to the required period and the nature and volume of the personal data, **as follows**:

Number of records for individuals' personal data	**Permit fee from 1 to 3 months (Egyptian Pounds)**	**Permit fee for more than 3 months to 6 months (Egyptian Pounds)**	**Permit fee for more than 6 months to 9 months (Egyptian Pounds)**	**Permit fee for more than 9 months to 1 year (Egyptian Pounds)**
From 1 to 25,000	Exempt from fees	Exempt from fees	Exempt from fees	Exempt from fees
More than 25,000 to 250,000	10,000 EGP	15,000 EGP	20,000 EGP	25,000 EGP
More than 250,000 to 500,000	12,500 EGP	25,000 EGP	37,500 EGP	50,000 EGP
More than 500,000 to 1 million	25,000 EGP	50,000 EGP	75,000 EGP	100,000 EGP
More than 1 million to 2 million	50,000 EGP	100,000 EGP	150,000 EGP	200,000 EGP
More than 2 million to 3 million	75,000 EGP	150,000 EGP	225,000 EGP	300,000 EGP

More than 3 million to 4 million	100,000 EGP	200,000 EGP	300,000 EGP	400,000 EGP
More than 4 million to 5 million	125,000 EGP	250,000 EGP	375,000 EGP	500,000 EGP
More than 5 million personal data records for individuals	The permit fee for any permit period shall be the maximum fee stipulated by law.			

- The fees for permits for controllers only or processors only for natural or legal persons shall be half the value indicated in the table above, according to the volume of data.

Article 21

(Conditions for Licensing Permit Controller and Processor from Legal Persons for Personal and Sensitive Personal Data)

The following is required to obtain a license/permit for controllers and processors from legal persons:

1. A statement of the mechanism used to obtain the consent of the data subject to the collection, retention, and processing of their data, as well as the mechanisms for exercising the data subject's legally stipulated rights.
2. Submitting proof of maintaining electronic records related to the controller's and processor's obligations.
3. Specifying the mechanisms and procedures used to secure and protect personal data in accordance with the security standards issued by the Center.
4. Submitting proof of the licensee's or permit holder's commitment to applying the provisions of the law and the terms of the license or permit, enabling the Center to inspect and monitor.

5. Submitting the contractual relationship document with the Personal Data Protection Officer, including explicit acceptance of the responsibilities of the Personal Data Protection Officer, and proof of the controller's or processor's commitment to granting the Personal Data Protection Officer the necessary independence to perform their duties.
6. Acknowledgment of commitment to the financial penalties imposed by the Center in the event of a violation of the terms of the license or permit.
7. Submitting proof of compliance with the controls and standards for handling sensitive personal data and children's data.

Article 22

(Conditions for Permitting Natural Persons' Controllers and Processors Personal and Sensitive Personal Data)

The following is required to obtain a permit for natural persons' controllers and processors:

1. A statement of the mechanism used to obtain the consent of the data subject on the collection, retention, and processing of his data, as well as the mechanisms for exercising the rights of the data subject as stipulated by law.
2. Identifying the mechanisms and procedures used to secure and protect personal data, in accordance with the security standards issued by the Center.
3. Providing evidence of the licensee's compliance with the provisions of the law and the terms of the license, enabling the Center to inspect and monitor.
4. Providing evidence of compliance with the controls and standards for handling sensitive personal data and children's data.

Article 23

(License or Permit for Cross-Border Transfer of Personal Data for Legal Entities)

The license or permit grants the controller or processor the right to transfer personal data collected or prepared for processing from within the geographical scope of the Arab Republic of Egypt to outside of it, in accordance with the controls and standards for cross-border handling of personal data contained in these regulations.

Article 24

(Conditions for Obtaining a License or Permit for Cross-Border Transfer of Personal Data for Legal Entities)

Without prejudice to the general conditions for obtaining a license or permit, the following is required to obtain a license or permit for the cross-border transfer of personal data for legal entities:

1. Specifying the destination to which the data is to be transferred.
2. Providing evidence of the nature of the activity of the controller or processor to whom the personal data is to be transferred.
3. Specifying the nature of the personal data being processed.
4. A statement of the security systems, temporary and final storage locations, and the procedures taken to protect the data during its transfer to the final destination.
5. Providing evidence of compliance with the standards, controls, and rules necessary for the transfer, storage, sharing, processing, or making data available across borders.
6. Specify the purpose of the cross-border data transfer.
7. Provide sufficient information about temporary and permanent storage locations according to the forms issued by the Center
8. Describe the categories of personal data transferred, their volume, and retention period.

Article 25 (Conditions for Obtaining a Permit for the Cross-Border Transfer of Personal Data of Natural Persons)

Without prejudice to the general conditions for obtaining a permit, the following conditions must be met to obtain a permit for the cross-border transfer of personal data of natural persons:

1. The nature and description of the personal data to be transferred across borders, its volume, and the purpose of the transfer.
2. Specifying the destination to which the data is to be transferred and the retention period.
3. A statement of the security systems, temporary and final storage locations, and the procedures taken to protect the data upon transfer to the final destination.

4. Providing evidence of compliance with the standards, controls, and rules necessary for the transfer, storage, or sharing of data across borders.
5. Specifying sufficient information about the temporary and final storage locations according to the forms issued by the Center.

Article 26

(Special Procedures for Obtaining a License or Permit for the Cross-Border Transfer of Personal Data of Legal and Natural Persons)

The representative of the legal or natural person submits an application to the Center to obtain a license or permit, as the case may be, to transfer personal data across borders through the designated electronic portal. The application must include all the data and documents referred to in Articles (24) and (25) of these Regulations.

The Center studies the application through specialized working groups, in accordance with the established procedures and rules, and may contact the applicant if any points need clarification or if any documents necessary for deciding on the application are required.

The Center informs the applicant of the outcome of the study, whether approval or rejection, within a period not exceeding 90 working days from the date of submission of all information and documents. Failure to respond is considered a rejection of the application.

Article 27

(Fees for Obtaining a License or Permit for Cross-Border Transfer of Personal Data)

The fees prescribed for obtaining a license or permit for the cross-border transfer of personal data shall be (50%) of the fees prescribed for obtaining a license/permit for a controller and/or processor, as applicable and according to the nature and volume of personal data.

Article 28

(License or Permit for Direct Electronic Marketing)

The license or permit shall be issued to the controller or processor, as applicable, who provides electronic marketing services.

This license or permit allows the use of personal data in the fields and activities of direct electronic marketing for oneself or others, in accordance with the legally prescribed terms and conditions.

Article 29

(Categories of Licenses/Permits for Direct Electronic Marketing)

The categories of licenses and permits for direct electronic marketing shall be determined as follows:

Category 1: License/Permits Related to Third-Party Direct Marketing: This license is issued to the controller and/or processor of third-party direct marketing service providers for the purpose of promoting the goods or services of third-party businesses.

Category 2: License/Permits Related to Self-Direct Online Marketing: This license is issued to the licensed controller and/or processor for the purpose of promoting the goods or services of their own business.

The fees for obtaining the special license/permit are determined for electronic marketing as follows:

The fee for a self-certified electronic marketing license or permit is 10% of the fee for a controller and/or processor license/permit. The fee for a third-party electronic marketing license or permit is 25% of the fee for a controller or processor license/permit.

Article 30

(Regulations for Obtaining a Direct Electronic Marketing License/Permit)

Obtaining an electronic marketing license or permit, in its various forms, is subject to the following regulations:

1. Submitting proof of obtaining approval from the competent authority to conduct the activity
2. Obtaining a controller or processor license/permit.
3. A statement of the mechanisms for obtaining the consent of the data subject to receive direct electronic communication regarding the product or service being marketed.

4. Specifying the mechanisms enabling the data subject to refuse electronic communication or withdraw their prior consent to receive such communication
5. Maintaining electronic records for recording the consents of the data subject with data and any requests for deletion or amendment thereto.

Article 31

(License to use visual surveillance equipment in public places)

The Center issues the license/permit for the use of visual surveillance equipment in public places, which would allow for the display or recording of images or videos of natural persons and their possession, and through which they can be identified**, in accordance with the following conditions**:

1. Obtaining the necessary licenses, permits and approvals from the competent authorities for the use of visual surveillance equipment in public places.
2. Publicly announcing the presence of visual surveillance equipment in visible locations.
3. Not transferring the availability/recording/processing of what has been monitored through these means to outside the geographical scope of the Arab Republic of Egypt except for reasons stipulated by law.
4. Not carrying out any processing that would access personal data through personal images or videos using technologies such as Face Recognition or other similar technologies, except in cases stipulated by law, or with the explicit consent of the data subject.
5. Taking the procedures and measures that obligate those in charge of operating visual surveillance systems in public places to maintain the confidentiality of this data and not use, circulate, or disclose it in any way, except for reasons stipulated by law.
6. Following the procedures and measures issued by the Center that ensure the security of recordings collected through visual surveillance equipment and protect them from hacking.

7. Enabling the Center to take the necessary monitoring and inspection measures on visual surveillance systems in public places to achieve its objectives and legally stipulated competencies.

- This excludes visual surveillance equipment used in individuals' residences, provided it does not exceed their spatial boundaries.

The fee for obtaining a license to use visual surveillance equipment in public places is 1,000 Egyptian pounds every three years, and the fee for obtaining a permit to use visual surveillance equipment in public places is 500 Egyptian pounds annually.

Article 32

(Conditions for obtaining accreditation to provide consultations on procedures for protecting the personal data of natural persons)

Conditions for obtaining accreditation to provide consultations on procedures for protecting the personal data of natural persons:

1. The applicant must possess academic qualifications or professional certificates, along with practical experience in relevant fields.
2. Passing the tests approved by the center according to the nature and size of the personal data activity for which registration is requested.
3. Must not have been previously convicted of any crime involving moral turpitude or dishonesty.

Article 33

(Requirements for obtaining accreditation to provide consulting services related to personal data protection procedures for legal entities)

The following are required to obtain accreditation to provide consulting services related to personal data protection procedures for legal entities:

1. Providing information that indicates the nature of the legal entity's activity and its basis.
2. Availability of practical experience in relevant fields

3. Submitting evidence that its employees in the field of consultations related to personal data protection procedures have obtained an accreditation certificate from the Center and a valid permit to practice in the field of consultations.

Article 34

(Fees for obtaining an accreditation certificate to provide consultations in the field of personal data protection for natural persons and legal entities)

The value of the prescribed fees for obtaining an accreditation certificate to provide consultations shall be as follows:

- For a natural person: Five thousand pounds annually.
- For a legal entity: Fifty thousand pounds annually.

The accreditation certificate is valid for three years from the date of issuance and is renewable for similar periods at the same fees mentioned.

Article 35

(Data and Documents Required to Obtain a License/Permit for Legal Entities)

To obtain a license/permit for legal entities, the following data and documents must be submitted:

1. A copy of the legal entity's commercial register, its address, legal representative, organizational structure, nature of activity, and contact information (telephone, email).
2. Specifying the category of license/permit required.
3. The nature and volume of personal data, and identifying sensitive data.
4. The retention period for personal data.
5. Specifying the security procedures for transferring personal data.
6. A statement of the mechanism for erasing and amending data according to the wishes of the data subject or for reasons stipulated by law.
7. Specifying the method of data storage.
8. Specifying the data protection officer.
9. A statement of the mechanism for obtaining the consent of the data subject

10. Providing all technical data on the infrastructure used, including (data center classification, types of equipment used, the company's current technical certificates and accreditations from various entities, and their compliance with the technical and operational requirements and obligations specified by the center).
11. Submitting the technical certificates and accreditations obtained by the license applicant regarding the security of personal data retention and processing, specifying the issuing authorities, the date of issuance, and their validity period.

Article 36

(Procedures for Obtaining Licenses and Permits for Legal Entities)

The Center issues licenses and permits for legal entities through an electronic portal established for the purpose of receiving applications for obtaining licenses and permits for legal entities, according to the following procedures:

1. An application for any of the licenses and permits specified in these regulations shall be submitted to the Center through the designated electronic portal. The application must include all the data and documents specified in these regulations for each category of licenses and fulfill any other requirements determined by the Center.
2. The Center shall study the application through specialized working groups, in accordance with the established procedures and rules. It may contact the applicant if any points need clarification or if any documents are required to decide on the application.
3. The Center shall inform the applicant of the outcome of the study, whether it is approval or rejection, within a period not exceeding 90 working days from the date of submission of all data and documents. Failure to respond shall be considered a rejection of the application.

Article 37

(Data and documents required to obtain a permit for natural persons)

To obtain a permit for natural persons, the following data and documents must be submitted:

1. A copy of the personal identification document, criminal record certificate, educational qualifications, and the nature of the work performed.
2. The nature and category of the permit requested.
3. The purpose of obtaining the permit.
4. The nature and volume of personal data being processed, and identification of sensitive data.
5. Specifying the retention period for personal data.
6. A statement of the mechanism for erasing and amending personal data according to the wishes of the data subject or for reasons stipulated by law.
7. Specifying the method of storing personal data.
8. A statement of the mechanism for obtaining and registering the consent of the data subject.
9. Completing all technical data on the infrastructure used, including the types of equipment used (current technical certificates and accreditations), and the extent of its compliance with the technical and operational requirements and obligations that must be met, as determined by the Center.
10. Submitting the technical certificates and accreditations obtained by the permit applicant regarding the security of the retention and processing of personal data, specifying the issuing authorities, the date of issuance, and their validity period.

Article 38

(Procedures of Obtaining Permits for Natural Persons)

The Center issues permit for natural persons through an electronic portal established for the purpose of receiving applications for obtaining permits for natural persons, according to the following procedures:

1. Applications for any of the permit categories specified in these regulations shall be submitted to the Center through the designated electronic portal. The application must include all data and documents specified in these regulations for each permit category and fulfill any other requirements determined by the Center.

2. The Center shall review the application through its specialized teams, in accordance with the established procedures and rules. It may contact the applicant if any points need clarification or if any documents are required to process the application.
3. The Center shall inform the applicant of the outcome of the study, whether approval or rejection, within a period not exceeding 90 days from the date of submission of all data and documents. Failure to respond shall be considered a rejection of the application.

In the event that the Center accepts the application, the permit for the natural person shall be for a period not exceeding one year, and he shall be responsible for implementing the provisions of the law and performing the duties of the data protection officer.

Article 39

(General Provisions and Conditions for Licenses and Permits for Legal and Natural Persons)

- Associations, syndicates, and clubs, when dealing with the personal data of their members and within the framework of their activities, are obligated to obtain the necessary licenses and permits in accordance with the controls and conditions stipulated in the law and these regulations.
- In the event that the number of personal data records exceeds the data for which the license or permit was issued, natural and legal persons must apply to the Center to amend the license/permit according to the nature, size, and categories of the data
- Legal entities wishing to obtain licenses or permits in accordance with the provisions of the law and these regulations are obligated to obtain the necessary approvals to conduct their activities.

Article 40

(Renewal of Licenses and Permits)

- **First - Renewal of Licenses:**

The license expires upon the expiry of its term and may be renewed for further periods upon a request submitted by the licensee to the Center according to the mechanisms it specifies, at least three months before the end of the license term.

Renewal shall be in accordance with the controls and conditions, and after payment of the prescribed fees for issuing the license.

- **Second - Permit Renewal:**

The permit expires upon the expiry of its term and may be renewed more than once by a request submitted by the permit holder to the Center according to the mechanisms it specifies, at least one month before the end of the permit's term.

Renewal shall be in accordance with the regulations and conditions and after payment of the prescribed fees for issuing the permit.

Article 41

(License/Permit/Accreditation Forms)

The forms for applying for licenses, permits, and accreditations shall be prepared electronically and submitted through an interactive platform via the Center's electronic portal.

The type of form, conditions, regulations, and procedures necessary for obtaining licenses, permits, and accreditations shall be determined in light of the nature of the applicant's activity and the data they select from the content registered on the platform. This includes all segments, categories, and levels related to the volume, nature, methods of storage and security of personal data, its purpose, and other standards, regulations, and measures that the Center's Board of Directors deems appropriate for protecting personal data.

The form shall be issued electronically after reviewing the requirements, documents, and necessary data for its issuance, including the following:

1. A statement of the type of personal data and the purpose for retaining or processing it.
2. A statement of the retention periods for personal data and the licensee's obligation to delete this data immediately upon the expiration of the specified purpose.
3. Proof that it maintains a special register of personal data that includes its categories, identifies those who will disclose or make available that data, the basis for this, and

the mechanisms it uses to delete or modify it, as well as any other data related to the transfer of personal data across borders.

4. Statement of the mechanism for obtaining the consent of the data subject
5. Acknowledgment of obligations related to the security of personal data
6. Acknowledgment of providing the necessary capabilities to enable the Center to inspect and monitor.
7. Acknowledgment by those dealing with the licensee of the guarantee of the confidentiality of personal data.
8. Acknowledgment of compliance with the financial penalties and compensations determined by the Center.

Best regards,

Translated by Shehata & Partners Law Firm

Tel: +2-010-2225-6100
E-mail: info@shehatalaw.com
Address: Cairo Business Plaza, New Cairo, Cairo, Egypt