مركز حماية البيانات الشخصية

PDPC

Personal Data Protection Center

Egypt’s Personal Data Protection Framework:

From Legal Foundations to Practical Compliance and Enforcement

Mar., 2026

Empowering Data Protection in Egypt: Regulatory Framework and Enforcement

1. Overview of Egypt's Personal Data Protection Law No. 151 of 2020
2. Personal Data Protection Center (PDPC): Roles and Responsibilities as the Regulatory Authority
3. Key Provisions and Highlights of the PDPL & its Executive Regulations
4. Compliance Toolkit Overview
5. Licenses/ Permits Applications
6. Application for Accreditation as Data Protection Consultant (DPC) / Data Protection Officer (DPO)

Overview of The Personal Data Protection Law

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

The Personal Data Protection **Law No. 151 of 2020 ("PDPL")** establishes a comprehensive framework for protecting personal data. The Law mandates the establishment of a Personal Data Protection Center **(“PDPC”)** as the competent authority **responsible for overseeing and enforcing compliance with the law.**

Key Elements of the PDPL:

- **Regulates** the collection, processing, storage, and transfer of personal data of Egyptian citizens, non-Egyptian residents, and Egyptians abroad
- **Ensures safeguarding of personal data** against unauthorized access, misuse, or disclosure
- **Prescribes limitations on processing** to ensure proportionate and respectful treatment of individual autonomy
- **Confers nine fundamental rights upon data subjects** to exercise control over their personal data

PDPC Roles and Responsibilities as the Regulatory Authority

- Article 19 of the Personal Data Protection Law mandates the establishment **of an economic authority, designated as the Personal Data Protection Center (“PDPC”).**

- PDPC’s mandate encompasses **the development and enforcement** of robust controls and mechanisms designed to govern the lifecycle of personal data, encompassing collection, processing, storage, transmission, dissemination, and any other handling of personal data, ensuring the rights of individuals and protecting them from any potential violations.

PDPC Roles and Responsibilities as the Regulatory Authority

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

The PDPC has a broad range of competences to fulfill its mandate, these include but are not limited to:

REGULATORY

1. Issuing licenses, permits, and accreditation
2. Registering Data Protection Officers (DPOs) and Personal Data Protection Consultants
3. Developing and setting the necessary policies, strategic plans, and programs for the protection of personal data)
4. Developing and applying decisions, controls, measures, procedures, and standards for the protection of personal data.
5. Expressing opinions on draft laws and international agreements that regulate personal data or relate to or reflect directly or indirectly on personal data.
6. Developing a guiding framework for codes of conduct for the protection of personal data and adopting codes of conduct for different entities.
7. Establishing controls on the movement of data across borders.

PDPC Roles and Responsibilities as the Regulatory Authority

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

The PDPC has a broad range of competences to fulfill its mandate, these include but are not limited to:

COMPLIANCE & ENFORCEMENT

1. Receiving and investigating complaints, and issuing the necessary decisions thereon.
2. Monitoring and inspecting those subject to the provisions of the law, and taking the necessary legal measures.

COORDINATION

1. Unifying policies and plans for the protection and processing of personal data within the Egyptian Republic.
2. Coordinate and cooperate with all governmental and non-governmental organizations and agencies in ensuring personal data protection measures.
3. Conclusion of agreements and memorandums of understanding, coordination, cooperation and exchange of experiences with international bodies.

PDPC Roles and Responsibilities as the Regulatory Authority

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

The PDPC has a broad range of competences to fulfill its mandate, these include but are not limited to:

AWARENESS & CAPACITY BUILDING

1. Supporting the development of the competence of personnel working in all governmental and non-governmental entities involved in the protection of personal data.
2. Organizing conferences, workshops, training, and educational courses, and issuing publications to raise awareness and educate individuals and entities about their rights regarding the handling of personal data.
3. Providing all types of expertise and consultations related to personal data protection.

Key Provisions and Highlights of the PDPL & Its Executive Regulations

A. Key concepts
B. Data Processing Principles
C. Data Subject Rights
D. Data Users’ Obligations

Key Provisions and Highlights of the PDPL & its Executive Regulations

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

A. PDPL Key Concepts (PDPL article 1):

- Personal Data
- Sensitive Personal Data
- Processing Data
- Data Subject
- Data Protection Officer(DPO)
- Personal Data Protection Consultant
- Data Users

Data Users

Understanding Your Role: Are you a controller or a processor?

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

◉ **Controller:** The controller is any natural or legal person who, by virtue of their profession or role, has the authority to **obtain** personal data and **determine the methods, procedures, and criteria for its storage, processing, and control**, in accordance with a specific purpose or activity.

*__Article 4 of the PDPL__ *provides for the role and responsibilities of the controller.*

◉ **Processor:** The processor is any natural or legal person who, by virtue of their profession or expertise, is authorized to process personal data **on behalf of the controller**, in accordance with an agreement and under the controller's instructions.

*__Article 5 of the PDPL__ *provides for the role and responsibilities of the processor.*

Understanding Your Role: Are you a controller or a processor?

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

- **Sector-Specific Examples of Controllers and Processors**

	Education	Ride hailing	Health	Mobile network services	Social media
Controller	A University's admission office is the controller when they collect and process personal data from applicants, such as names, addresses, and grades, to decide who gets accepted..	A ride-hailing service provider is the controller when they collect and process personal data from drivers and passengers, such as names, phone numbers, and locations, to facilitate rides and manage their service.	A hospital is the controller when they collect and process personal health data from patients, such as medical histories and test results, to provide medical care and manage treatment.	A mobile network operator is the controller when they collect and process personal data from subscribers, such as call records and location data, to provide mobile services and manage accounts.	A social media platform is the controller when they collect and process personal data from users, such as names, emails, and browsing history, to provide services and target advertising
Processor	A company providing student information systems is the processor when they process personal data of students, such as enrollment and academic records, on behalf of schools (controllers).	A company providing mapping and navigation services is the processor when they process location data and ride history on behalf of ride-hailing companies (controllers).	A company providing medical transcription services is the processor when they process personal health data, such as doctor-patient conversations and medical test results, on behalf of hospitals and clinics (controllers).	A company providing customer relationship management (CRM) services is the processor when they process personal data, such as customer complaints and service requests, on behalf of mobile network operators (controllers).	A company providing content moderation services is the processor when they process personal data, such as user posts and comments, on behalf of social media platforms (controllers).

Key Provisions and Highlights of the PDPL & its Executive Regulations

B. Data Subject Rights (PDPL Article 2)

The PDPL establishes **nine fundamental rights for data subjects**

- Right to be Informed
- Right of Access
- Right of Withdrawal
- Right of Rectification
- Right to Erasure
- Right to Restrict
- Right to be Notified in case of Data Breach
- Right to Object
- Right of Portability

Key Provisions and Highlights of the PDPL & its Executive Regulations

C. Data Processing Principles (PDPL Article 3):

The PDPL sets out **seven data processing principles**

- **Lawfulness and Transparency**
- **Purpose Limitation**
- **Data Minimization**
- **Data Accuracy**
- **Storage Limitation**
- **Integrity and Confidentiality**
- **Accountability**

Key Provisions and Highlights of the PDPL & its Executive Regulations

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

D. Data Users' Obligations (PDPL Articles 4 & 5) - (ER-PDPL Articles 3 & 4) :

The PDPL & its Executive Regulations provide **the roles and responsibilities of controllers and processors, some of which are presented below.**

- Not disclosing personal data
- Appointing a DPO
- Applying for the relevant Licenses/ Permits
- Data Breach Notification
- Sensitive Personal Data Obligations/Children's Data Obligations
- Cross-Border Obligations
- Direct Marketing Obligations
- VMS in public spaces Obligations
- Appointment of a Representative in Egypt

Key Provisions and Highlights of the PDPL & its Executive Regulations

Not disclosing personal data

- **Responsibilities in Ensuring Non-Disclosure of Personal Data, but not limited to:**
  - Overseeing the implementation and effectiveness of policies and procedures governing the non-disclosure of personal data.
  - Monitoring the application of technical and organisational security measures, including access controls and role-based authorization.
  - Ensuring the establishment and delivery of awareness and training programs related to confidentiality and unauthorised disclosure.
  - Reviewing and monitoring audit, logging, and incident reporting mechanisms related to personal data disclosure.

Key Provisions and Highlights of the PDPL & its Executive Regulations

Appointing a DPO

❑ Determining the Appropriate DPO for the Organisation

- ➢ Assess the nature and sensitivity of the personal data processed by the organisation
- ➢ Consider the volume of personal data.
- ➢ Review the scope, purposes, and complexity of processing activities carried out
- ➢ Based on the above assessment, determine which category of DPO is appropriate to serve the organisation
- ➢ Ensure that the appointed DPO's qualifications and role are proportionate to the organisation's data processing risks and obligations

Key Provisions and Highlights of the PDPL & its Executive Regulations

❑ Requirements for DPO Appointment

Appointing a DPO

- The DPO role shall be explicitly reflected in the entity's organizational chart.
- To ensure independence, the DPO shall report directly to the highest management level.
- The DPO may be engaged through an employment agreement or a service contract.
- The DPO may be an existing employee, a new hire, or an external appointment. Where a single DPO is intended to serve multiple controllers, approval from the PDPC and all relevant controllers is mandatory
- The DPO can be an existing employee of the organization, and they may continue to perform their previous duties alongside the DPO role so long as the condition of independence is met and that the PDPC has approved the role during the registration process.
- The DPO can be either an Egyptian national or a foreigner, but they must be registered with the PDPC in order to serve in this role.
- The DPO must be independent and should not be involved in decision-making regarding processing activities relevant to personal data.

Key Provisions and Highlights of the PDPL & its Executive Regulations

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

Appointing a DPO

❑ DPO Categories in PDPC Registry

PDPC Registry recognizes **three categories of DPOs:**

Category A (Lead DPO)	Category B (Advanced DPO)	Category C (Entry-Level DPO)
Highly experienced DPOs with advanced expertise in data protection	Competent DPOs with solid knowledge and practical experience in data protection or a related field	Entry-level DPOs with foundational knowledge in data protection or a related field

PDPC will categorize DPOs based on existing certifications, such as those offered by the International Association of Privacy Professionals **(IAPP)** and other reputable international organizations, as well as its exams for each category.

Key Provisions and Highlights of the PDPL & its Executive Regulations

❑ Licensing Obligations When Processing Personal Data

Applying for the relevant Licenses/ Permits

- Where an entity processes personal data, it shall obtain the license/permit for processing personal data as a controller and/or processor, which constitutes the mandatory and core license in all cases.
- The entity shall assess the need to obtain additional licenses/permits, such as:
  - Direct electronic marketing
  - Cross-border transfer of personal data
  - Use of visual surveillance systems in public places
- The entity shall assess the volume of personal data records processed to determine the applicable license or permit category. (1 record = 1 Data Subject)
- The entity shall determine whether the processing activity is occasional or ongoing, where:
  - Occasional processing activities require a permit;
  - And ongoing processing activities require a license.
- The entity shall ensure the appointment of a Data Protection Officer (DPO) as a prerequisite for obtaining the relevant license or permit.
- Prior to submitting any license or permit application, the entity should implement a data protection compliance plan to assess its compliance with the provisions of the Law and its Executive Regulations.

Key Provisions and Highlights of the PDPL & its Executive Regulations

Appointment of a Representative in Egypt

- Where an entity does not have an establishment within the Arab Republic of Egypt and processes personal data relating to Egyptian data subjects or data subjects resident in Egypt, such entity shall appoint a legal representative in Egypt.

- Data Users may choose among several forms of representations through existing legal entities, offices and/or individuals, provided that the designation is submitted to PDPC for examination and approval.

- The approved legal representative shall act as the entity's official interface with PDPC.

Key Provisions and Highlights of the PDPL & its Executive Regulations

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

Data Breach Notification

- **Risk Assessment and Impact Analysis**
  - Assess the nature of the breach or violation, the type of personal data affected, and the potential risks and impacts on data subjects.
- **Incident Response Plan Activation**
  - Activate the approved incident response procedures to contain the breach, mitigate its effects, and document corrective and security measures taken.
- **Breach Awareness and Notification**
  - Notify PDPC within seventy-two (72) hours from the date of becoming aware of the breach.
  - Where the breach is related to national security considerations or the entities responsible therefor, notification to PDPC shall be made immediately.
  - Data subjects shall be notified within three (3) working days from the date of notifying PDPC
- **Post-Incident Measures and Follow-Up**
  - Implement remedial and preventive measures, update internal controls and procedures, and retain documentation related to the breach, notifications, and corrective actions.

Key Provisions and Highlights of the PDPL & its Executive Regulations

Sensitive Personal Data Obligations/Children's Data Obligations

❑ Obligations When Processing Sensitive Personal Data

- ➢ The controller shall obtain explicit written consent when processing sensitive personal data.
- ➢ Explicit consent can be obtained in physical or electronic form.

❑ Obligations When Processing Children's Personal Data

- ➢ Children under 15 years of age: **The controller shall obtain the explicit written consent of the parent or legal guardian** prior to collecting or processing the child's personal data, and such consent shall clearly specify the purpose and duration of the processing.

- ➢ Children aged 15 to 18 years: **They may submit to the controller the explicit written consent of the legal guardian** for the collection and processing of their personal data, and such consent shall clearly specify the purpose and duration of the processing.

Key Provisions and Highlights of the PDPL & its Executive Regulations

Cross-Border Obligations

- Articles 14, 15, and 16 of the PDPL, as well as Article 16 of the ER-PDPL, stipulate the requirements and conditions for the legitimate transfer of personal data across international borders.

- **Key Requirement:**
  - Identify the categories of personal data transferred, distinguishing between data in transit and data at rest, and mapping transfer routes, recipients, and locations.
  - Perform a Transfer Impact Assessment (TIA) covering risks to data subjects and the adequacy of safeguards.
  - Assess the data protection framework of the destination jurisdiction, including the existence of a data protection authority and applicable data protection legislation.
  - Assess the recipient entity and any dependent or affiliated entities to ensure compatibility in joint or integrated processing operations and the existence of a legitimate interest for the parties and/or the data subject.
  - Ensure the availability of effective remedial measures and enforceable rights for data subjects in the destination jurisdiction.
  - Ensure the application of appropriate technical and organisational security measures for cross-border personal data transfers.
  - Ensure contractual arrangements governing the cross-border transfer are in place in a manner that ensures compliance with the PDPL and its Executive Regulation.
  - Prior authorisation or approval from PDPC is required (License/Permit)

Pursuing Adequacy and Alternative Mechanisms for Secure Cross-Border Data Transfers

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

	Adequacy Decision	Appropriate Safeguards
Cross- Border Data Transfers Mechanisms	Adequacy decision refers to a formal determination that a country, territory, sector, or organization provides a sufficient level of protection for personal data, enabling the transfer of data without additional safeguards. PDPC will maintain a whitelist of countries deemed to have an adequate level of personal data protection, equivalent to that of Egypt. This whitelist will facilitate the transfer of personal data between Egypt and these countries, without the need for additional safeguards.	1. **Standard Contractual Clauses (SCCs)**: Approved clauses by PDPC. 2. **Binding Corporate Rules (BCRs)**: Regulations adopted by multinational businesses, enabling group international data transfers while ensuring consistent data protection levels. 3. **Agreements**: Agreements for cross-border data transfers between entities. Examples: Data processing agreements, data transfer agreement ..etc. 4. **Codes of Conduct**: Approved codes of conduct created by associations and businesses, specifying PDPL application and cross-border data transfer procedures.

Key Provisions and Highlights of the PDPL & its Executive Regulations

Direct Marketing Obligations

- Articles 17 and 18 of the PDPL, as well as Article 18 of the ER-PDPL, stipulate the requirements and conditions for legitimate Electronic Digital Marketing practices.

- **Key Requirements**:
  - Prior authorization or approval from PDPC is required (License/Permit)
  - Explicit Consent
  - Easy Withdrawal Mechanisms
  - Transparency

Key Provisions and Highlights of the PDPL & its Executive Regulations

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

VMS in public spaces Obligations

- Pursuant to Article 26 of the PDPL, any entity operating a visual surveillance system that processes personal data is required to obtain a license or permit from the PDPC. In this context, Article 31 of the ER-PDPL governs the lawful, controlled, and licensed use of visual surveillance systems in public places.

- **Key Requirement:**
  - Prior authorization or approval from PDPC is required (License/Permit)
  - Prior approvals from competent authorities must be obtained.
  - A clear and visible notice of the use of visual surveillance systems must be provided.
  - Processing or transfer of surveillance data outside Egypt is prohibited, except for legally prescribed reasons.
  - There must be a lawful basis or explicit consent of the data subject for the use of facial recognition or similar technologies.
  - Confidentiality and security measures must be implemented to prevent unauthorised use, disclosure, or access to recordings.
  - Exemption applies to private residential premises, provided surveillance does not extend beyond the premises.

Compliance Toolkit Overview

1. Establishing Compliance Foundations

- Conducting a Readiness Assessment
- Understanding Your Role: Are you a controller or a processor?
- Appointing a Data Protection Officer (DPO)

2. Compliance with Key Provisions

- Data Processing Principles
- Lawful Basis
- Consent Management
- Cross-Border Data Transfers
- E-Marketing
- Visual Monitoring Systems (VMS)
- Breach Notification
- Data Subject Requests
- Cloud Computing and Data Centers

3. Operationalizing Data Protection

- A Structured Approach to Privacy Management: Assess, Protect, Sustain, Respond

Compliance Starts Here!

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

- ✓ Identify and document the personal data collected
- ✓ The purpose of the collection
- ✓ The level of control exerted over its processing
- ✓ Review responsibilities and obligations under the PDPL, ER, and PDPC guidelines
- ✓ Conduct a gap analysis

Launch of License/ Permit Application Services via the PDPC Portal

- ✓ **Access the Personal Data Protection Center's website at pdpc.gov.eg**
- ✓ **Create an account on the portal**
- ✓ **Select and initiate the relevant service**
- ✓ **Complete the required questionnaire**
- ✓ **Appoint a Data Protection Officer (DPO)**
- ✓ **Submit the application together with all required supporting documents**

Application for Accreditation as Data Protection Consultant (DPC) / Data Protection Officer (DPO)

مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

Launch of DPC/ DPO Accreditation Application Services via the PDPC Portal

- **Data Protection Officer (DPO) Accreditation:**
  - ✓ **Create** an account on the portal
  - ✓ **Select** the relevant category
  - ✓ **Complete** the category-specific examination
  - ✓ **Request** the DPO registration service
  - ✓ **Select** the category for registration
  - ✓ **Upload** the required supporting documents
  - ✓ **Submit** the application

- **Personal Data Protection Consultant (DPC) Accreditation:**
  - ✓ **Create** an account on the portal
  - ✓ **Select** the Personal Data Protection Consultant (DPC) accreditation service
  - ✓ **Submit** the required documents

THANK YOU!