IPA
Influence Public Affairs

EXECUTIVE ANALYTICAL BRIEF ON

Egypt's Personal Data Protection Executive Regulations

FEB 2026

EXECUTIVE SUMMARY

This paper examines the Executive Regulations of the Egyptian Personal Data Protection Law No. 151 of 2020, issued by Ministerial Decision No. 86 of 2025 and **published in the Official Gazette on 1 November 2025**, which formally entered into force as the governing framework for the implementation of personal data protection in Egypt. It forms part of a broader analytical examination of recent legislative and regulatory developments in this field, approaching the Executive Regulations as a legal and regulatory instrument in their own right.

The issuance of the Executive Regulations constitutes a decisive phase in the operationalization of the Personal Data Protection Law, insofar as they translate the law's general principles into detailed and binding procedural rules governing the collection, processing, storage, disclosure, transfer, and protection of personal data throughout its full lifecycle. Beyond proceduralization, the Regulations articulate the institutional architecture of the data protection regime by defining the roles of **the Personal Data Protection Center**, establishing compliance obligations for regulated entities, and setting out supervisory, licensing, and enforcement mechanisms that give the statutory framework practical and operational effect.

With the official entry into force of the Executive Regulations, the regulatory system governing personal data protection in Egypt has moved from a predominantly normative phase to one of concrete application. This transition necessitates a systematic and **text-based review** of the Regulations themselves as the primary reference for compliance, oversight, and enforcement. Accordingly, this paper examines the executive framework on its own terms.

The paper therefore offers a structured and **comprehensive analytical reading of the Executive Regulations**, identifying their principal regulatory pillars, substantive obligations, and implementation tools. This analysis is intended to serve as a neutral and doctrinal reference that contributes to a clearer understanding of the executive framework, elucidates the regulatory architecture it establishes.

GENERAL OVERVIEW OF THE EXECUTIVE REGULATIONS

The Executive Regulations of Egypt's Personal Data Protection Law constitute the primary instrument for operationalizing **Law No. 151 of 2020**, translating its broadly framed legal principles into an enforceable procedural and regulatory architecture. Rather than introducing new substantive rights or obligations, the Regulations are structured to organize the application of the law through detailed administrative, technical, and supervisory mechanisms governing the handling of personal data across its entire lifecycle.

At their core, the Regulations adopt a lifecycle-based regulatory approach, addressing personal data from the point of collection and processing, through storage, security, use, disclosure, and availability, and ultimately to transfer within or outside the Arab Republic of Egypt. This approach is accompanied by a strong centralization of regulatory authority, whereby the competent center is positioned as the primary body responsible for licensing, oversight, approval mechanisms, and the issuance of technical and organizational standards. Through this design, the Regulations seek to consolidate regulatory control over data protection practices while maintaining flexibility through delegated rulemaking.

The Executive Regulations rely on a set of foundational compliance instruments. These include:

- **Mandatory record-keeping obligations for controllers and processors**
- **Formalized consent frameworks with documentation requirements**
- **Structured procedures for personal data breach notification**.

A notable feature of the Regulations is their extensive treatment of the Personal Data Protection Officer (DPO) role. Rather than focusing on liability or sanctions, the Regulations emphasize the **professionalization** and **institutional embedding** of the DPO function. They establish detailed requirements concerning registration, qualifications, competencies, duties, reporting lines, and conflict-of-interest safeguards, signaling an intent to integrate the DPO as a formal compliance actor within organizational governance structures.

The Regulations also introduce differentiated safeguards for categories of data deemed to require heightened protection. Sensitive personal data are subject to stricter consent requirements and additional limitations on processing, reflecting a regulatory assessment that certain data categories carry inherently higher risks and therefore warrant enhanced procedural protections.

GENERAL OVERVIEW OF THE EXECUTIVE REGULATIONS

From a cross-border perspective, the Regulations provide a structured framework governing **international personal data transfers.** This framework is based on prior licensing or authorization, coupled with an assessment of the level of protection afforded by recipient jurisdictions or entities. By subjecting cross-border transfers to notification and ongoing oversight, the Regulations embed international data flows within a centralized approval regime.

In parallel, the Regulations establish a comprehensive **licensing and fee regime**. The fee structure is anchored primarily to quantitative criteria, most notably the number of personal data records, rather than to financial metrics such as revenue size or sectoral classification. This choice reflects a regulatory emphasis on data volume and risk exposure as the principal determinants of compliance cost.

Within this framework, the Regulations distinguish between licenses limited to non-sensitive personal data and those involving sensitive personal data, indicating a differentiated regulatory treatment. However, while the Regulations explicitly recognize that licenses involving sensitive data fall under a distinct scope with higher regulatory weight, **they do not provide a standalone numerical fee schedule or calculation methodology for such data**. Instead, the determination of applicable costs is deferred to subsequent executive decisions and guidelines issued by the competent authority, reinforcing the role of secondary regulation in completing the compliance framework.

Taken as a whole, the Executive Regulations are primarily oriented toward establishing the procedural, institutional, and supervisory foundations necessary for the effective application of the Personal Data Protection Law. At the same time, they deliberately leave a number of substantive and operational matters to be addressed through future regulatory instruments. In this sense, the Regulations should be understood as a foundational regulatory phase designed to enable enforcement and oversight.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

1) ARTICLES 2 & 3(8): CONTROLLER OBLIGATIONS IN LIGHT OF SECTOR-SPECIFIC REGULATIONS

Articles (2) and (3) of the Executive Regulations establish **the foundational procedural** and **operational obligations** governing the collection, processing, retention, and protection of personal data. Rather than framing these obligations in isolation, the provisions embed data protection compliance within a broader regulatory environment shaped by sector-specific legal frameworks. This is particularly evident in the procedural requirements under Article (2), and in the language of Article (3)(8), which explicitly links controller obligations to the legal limits imposed by the laws regulating the controller's core activity.

Article (2), particularly under the section on "procedures and policies," introduces a structured compliance architecture that requires controllers to institutionalize data governance internally. It obliges entities to inform data subjects of their rights, **adopt security programs and technical safeguards issued by the Center**, and maintain a secured electronic record documenting key aspects of data processing.

These records must include, among other elements:

- **Documented consent**
- **The categories of personal data collected**
- **The scope of their use**
- **The protection measures adopted**

This procedural layer reflects an approach that treats data protection as an internal governance function embedded within institutional operations. Controllers are required not only to obtain consent and apply security safeguards, but also to formalize compliance through documentation, internal policies, and systematic record-keeping. The emphasis on structured procedures suggests that compliance is expected to operate continuously, rather than as a one-time licensing condition.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

1) ARTICLES 2 & 3(8): CONTROLLER OBLIGATIONS IN LIGHT OF SECTOR-SPECIFIC REGULATIONS

Article (3) complements this framework by setting out the broader obligations of controllers. Within this structure, paragraph (8) carries particular significance. It requires the controller to limit the volume and type of personal data obtained to **what is permitted under the law governing its primary activity**. It further provides that, where **the sector-specific law regulating that activity** does not itself contain rules on the collection, retention, transfer, or protection of personal data, the general rules established by the Personal Data Protection Law and its Executive Regulations shall apply to any additional personal data requested or processed.

This provision effectively establishes a layered compliance model. Controllers are first bound by the legal limits defined in the legislation governing their sectoral activity, such as financial, telecommunications, healthcare, or other regulated fields. Where those laws specify the scope of data collection, that scope defines the baseline. Where they are silent on data protection standards, the Executive Regulations step in as the default regulatory framework governing storage, security, and transfer.

From a regulatory design perspective, this creates a **dual-reference compliance structure**. The controller's obligations are not determined solely by the data protection regime, but also by the substantive legal framework of the activity through which the data is collected. Article (3)(8) thus operates as a bridging provision that connects sectoral legislation with the data protection framework, ensuring that data processing remains anchored in the lawful scope of the underlying activity while extending general protection rules where sector-specific legislation does not provide them.

When read together, Article (2) (procedures and policies) and Article (3)(8) reveal a governance model based on institutional responsibility and regulatory layering. The result is a compliance architecture in which personal data protection is not treated as a stand-alone obligation, but as one that interacts with and is shaped by the legal regime governing the controller's core activity

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

2) ARTICLES 7 - 12: PERSONAL DATA PROTECTION OFFICER (DPO) AND INSTITUTIO RESPONSIBILITY

Law No. 151 of 2020 positions the Personal Data Protection Officer (DPO) as a key element of the personal data protection framework, assigning to this role specific duties related to monitoring compliance and ensuring the lawful processing of personal data. The legal construction of this role culminates in Article (40) of the Law, which establishes a distinct liability regime applicable directly to the DPO in his or her individual capacity.

Regulatory Structuring of the DPO Role:

Against this statutory backdrop, the Executive Regulations approach the DPO from a fundamentally different angle. Rather than engaging with questions of liability or sanctions, the Regulations focus on organizing the role as a regulated professional function within entities subject to the Law.

Articles (7) to (12) of the Executive Regulations collectively set out a procedural and administrative framework governing the DPO's appointment, registration, qualifications, and scope of practice. Articles (7) and (8) establish the technical and legal qualifications required for registration with the Personal Data Protection Center, while Article (9) creates an official registry for DPOs, placing the role under centralized regulatory supervision.

The Regulations further delegate to the Center, under Article (10), the authority to determine the specific competencies of the DPO through subsequent decisions, taking into account the nature and scale of the entity's activities. This provision emphasizes regulatory flexibility but does not itself allocate decision-making authority or managerial responsibility to the DPO.

Articles (11) regulate matters related to termination, replacement, and conflicts of interest, including the permissibility of serving multiple entities with the Center's approval. Article (13) defines the DPO's operational obligations, such as monitoring compliance, coordinating with controllers and processors, cooperating with the Center, and preparing periodic compliance reports.

Notably, none of these provisions introduce enforcement mechanisms or refer back to the liability regime established in Article (40) of the Law.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

2) ARTICLES 7 - 12: PERSONAL DATA PROTECTION OFFICER (DPO) AND INSTITUTIO RESPONSIBILITY

Institutional Responsibility:

A consolidated reading of the Executive Regulations reveals a clear regulatory choice: while the DPO's role is extensively structured from a professional and procedural perspective, the Regulations do not allocate responsibility to senior management, boards of directors, or other executive bodies for compliance failures. Nor do they reinterpret or contextualize the individual liability imposed on the DPO under the Law.

As a result, the liability regime applicable to the DPO remains anchored exclusively in the statutory text, operating independently of the regulatory framework that governs the practical execution of the role. The Executive Regulations neither dilute nor supplement the individualized liability model established by Article (40) of Law No. 151 of 2020, leaving questions of institutional accountability unaddressed at the regulatory level.

The Executive Regulations institutionalize the DPO as a registered and supervised compliance function, while the Law alone governs the consequences of non-compliance through direct sanctions imposed on the individual officer.

3) ARTICLES 14 AND 15: HANDLING OF SENSITIVE PERSONAL DATA

Articles (14) and (15) establish a stricter regulatory framework for the processing of sensitive personal data, reflecting its higher risk nature and the need for enhanced safeguards. Article (14) requires controllers and processors to obtain a special permit from the Personal Data Protection Center before processing sensitive data, in addition to securing explicit written consent from the data subject or from a legal guardian in the case of children. Processing must be limited to data that is strictly necessary for the stated purpose, and entities must comply with the technical and security standards set by the Center.

The provision includes additional protections for children, particularly by prohibiting the publication or use of children's data in profiling or behavioral monitoring contexts.

Article (15) complements this framework by setting specific rules for children's data. It requires prior written consent from a parent or guardian before collecting data relating to individuals under 18. For those aged 15 to 18, the controller must also inform both the child and the guardian about the nature and purpose of the data processing.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

4) ARTICLES (16) AND (17): CROSS-BORDER DATA TRANSFERS

Articles (16) and (17) establish the regulatory framework governing the transfer, storage, sharing, and availability of personal data across borders, with a focus on ensuring that personal data originating in Egypt remains subject to adequate protection when processed abroad.

Article (16) sets the core legal and procedural conditions for cross-border data movement. As a general rule, controllers and processors may not transfer, store, or share personal data outside Egypt without obtaining prior authorization from the Personal Data Protection Center. The provision requires entities to implement appropriate technical and organizational safeguards to protect confidentiality and integrity during transfer or storage abroad.

Particularly significant is **the second section of Article (16)**, which introduces policy-based standards for assessing whether a foreign jurisdiction provides an adequate level of protection. **These include:**

The Center must confirm that the destination jurisdiction or entity offers a level of protection consistent with the requirements of Egyptian law before granting authorization.

Article (17) complements this framework by regulating the disclosure of personal data to another controller or processor, whether inside or outside Egypt, in exceptional cases and subject to prior licensing. The provision recognizes situations such as intra-group data sharing within corporate structures or joint contractual arrangements, provided that the level of protection remains equivalent to that required domestically.

Together, these provisions establish a compliance driven model for cross-border data governance based on prior authorization, adequacy assessment, and continuous responsibility on controllers and processors to ensure that transferred data remains protected in accordance with national legal standards.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

5) ARTICLES (19) AND (20): LICENSING AND FEES

The Executive Regulations of the Personal Data Protection Law establish a comprehensive licensing and fee regime governing activities related to the control and processing of personal data. This regime, as set out primarily in Articles (19) and (20), adopts a graduated regulatory model based on two core variables: the volume of personal data records and the scope of the licensed activity.

Structure of the Licensing Framework

Article (19) sets out the foundational structure of the licensing system, defining the activities subject to licensing and establishing the principle that licensing obligations are assessed according to the number of personal data records processed or controlled. The provision reflects a quantitative regulatory approach, whereby licensing requirements and associated fees are determined by data volume rather than by economic indicators such as revenue size, sector classification, or legal form of the regulated entity.

This design choice positions the licensing framework as a technically driven regulatory mechanism focused on the scale of data processing operations, rather than on broader business or market considerations.

Fee Thresholds and Graduated Structure

Article (19) operationalizes the licensing framework by introducing a graduated fee structure linked to specific data-record thresholds. The Executive Regulations establish the following milestones:

Personal Data Records Scope	Prescribed Fees
Up to 100,000 records	Full exemption from licensing fees
101,000 to 1 million records	Gradual increase up to approximately EGP 1,000 annually
1,000,001 to 5 million records	Gradual increase up to approximately EGP 500,000 annually
5 million records or more	Maximum annual fee of EGP 666,666; (three-year license to be issued at EGP 2 million)

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

5) ARTICLES (19) AND (20): LICENSING AND FEES

This graduated structure reflects an explicit regulatory intent to scale financial obligations in proportion to the quantitative footprint of personal data processing activities, while maintaining fixed upper limits on licensing fees.

Distinction in Licensing Fee Structure

Articles (19) and (20) of the Executive Regulations establish a tiered licensing fee model that functions as a graduated compliance mechanism. Smaller-scale processing activities benefit from exemptions or relatively modest licensing costs, while entities operating at higher data volumes are subject to progressively higher fees. This structure signals an intention to proportion regulatory cost to the breadth of data-handling activity, thereby aligning financial obligations with the potential administrative and supervisory burden placed on the regulatory authority.

Temporary Permits Regime

Article (20) further introduces a separate regulatory regime for temporary permits applicable to controllers and/or processors operating for limited durations. These permits are subject to defined issuance and renewal fees and may be granted for periods not exceeding five years. The Article also empowers the competent authority to refuse, suspend, or withdraw permits in cases of non-compliance with regulatory requirements.

Under this regime:

- Initial permit fees start at EGP 10,000 for smaller entities.
- Fees rise progressively to EGP 500,000 for entities processing more than one million personal data records.
- Renewal fees are set at levels lower than initial issuance fees.

Taken together, Articles (19) and (20) reveal a licensing and fee regime grounded in administrative measurability and regulatory predictability, prioritizing data volume and data sensitivity as the primary determinants of financial obligations.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

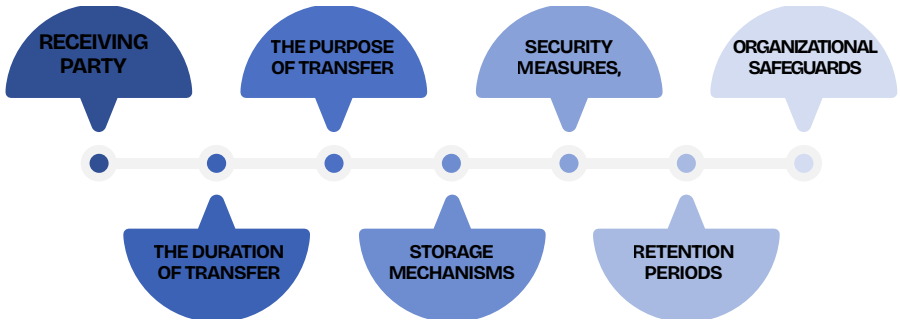
6) ARTICLES 23–27: CROSS-BORDER DATA TRANSFER LICENSING FRAMEWORK

Articles (23) to (27) establish a structured regulatory regime governing the licensing and authorization required for transferring personal data outside the Arab Republic of Egypt. Together, these provisions move beyond general principles and introduce a detailed compliance framework that regulates both the substantive conditions and procedural requirements for lawful cross-border data movement.

Article (23) sets the general rule that any transfer of personal data collected within Egypt to entities abroad—whether by a controller or processor—**requires prior approval from the Personal Data Protection Center**, in accordance with the standards and safeguards established in the Executive Regulations. This provision reinforces the central supervisory role of the Center in authorizing cross-border processing activities.

Articles (24) and (25) differentiate between legal persons and natural persons in terms of licensing requirements.

For legal entities, the application must specify the following:



For natural persons, similar requirements apply, including:

- Clarification of the type and volume of data
- The purpose, duration of transfer and storage systems,
- The security procedures adopted

These provisions collectively demonstrate a risk-management approach, placing emphasis on traceability, purpose limitation, and demonstrable protection standards.

ANALYSIS OF KEY PROVISIONS IN THE EXECUTIVE REGULATIONS

6) ARTICLES 23–27: CROSS-BORDER DATA TRANSFER LICENSING FRAMEWORK

Article (26) introduces a procedural layer, requiring applications to be submitted through designated forms accompanied by supporting documentation. It also grants the Center the authority to request additional information within a defined review period, with the absence of a response constituting a rejection. This reflects a formal administrative licensing model based on documentation, verification, and discretionary approval.

Article (27), however, carries particular practical significance, as it determines the financial dimension of cross-border data compliance. The provision stipulates that the fee for obtaining a license or permit for cross-border data transfer shall be set at 50% of the applicable licensing fees for controllers and/or processors, depending on the nature and volume of the data. This effectively links cross-border transfer costs directly to the broader licensing structure governing data processing activities.

This provision signals a regulatory intent to treat cross-border data transfers as an extension of core data processing operations rather than as an independent activity. At the same time, by tying the cost to underlying processing licenses, it introduces an additional financial layer that organizations must factor into compliance planning, particularly those engaged in multinational operations or cloud-based data architectures.

For businesses, this framework has several practical implications. First, cross-border transfer is not merely a technical or operational matter but a regulated activity requiring prior authorization and documented safeguards. **Second, the cost structure particularly the 50% fee model under Article (27)** means that entities already subject to licensing as controllers or processors must anticipate additional compliance expenses when transferring data internationally. Third, the documentation-heavy application process suggests the need for strong internal governance mechanisms capable of demonstrating purpose limitation, storage controls, and technical security measures.

CONCLUDING REMARKS

The issuance of the Executive Regulations marks a substantive step toward operationalizing Egypt's personal data protection framework and provides a foundational procedural structure for implementation. The Regulations have addressed several core organizational and financial dimensions, particularly in relation to licensing mechanisms for non-sensitive personal data and the establishment of supervisory and registration systems.

In light of these observations, the following recommendations are proposed from a business and institutional compliance perspective, focusing on internal readiness, governance strengthening, and proactive engagement with the regulatory environment:

- Businesses should invest in structured internal coordination mechanisms to manage data protection responsibilities across departments to maintain consistency in interpretation and application of regulatory obligations.

- Senior management awareness and engagement should be strengthened through targeted training programs. Executive leadership plays a critical role in embedding data protection within institutional governance, and supporting compliance functions.

- The role of the Personal Data Protection Officer (DPO) should be reinforced at the organizational level by clearly defining reporting lines, responsibilities, and decision-making authority within internal governance structures. Regular training for DPOs and compliance teams should be prioritized to ensure familiarity with evolving regulatory expectations and sector-specific requirements.

- Businesses should maintain proactive and continuous coordination with the Personal Data Protection Center, including early consultation when introducing new processing activities, adopting new technologies, or expanding cross-border operations.

- For entities engaged in cross-border data operations, it is advisable to develop internal protocols governing data transfer decisions, including documentation of transfer purposes, storage locations, security safeguards, and retention periods.

- Businesses should consider engaging specialized data protection consultants or expert agencies to support the early phases of compliance, through structured training programs for senior management and the Personal Data Protection Officer (DPO), alongside providing continuous advisory support, regulatory interpretation, and practical guidance to help build internal capacity and ensure informed decision-making as the organization adapts to the evolving data protection framework.

IPA
Influence Public Affairs

Established in 2015 as the strategic arm of Influence Communications Group, a prominent marketing communications consultancy since 2007, IPA has become a leading public policy and public affairs firm, supporting over 90 clients across local and regional markets.

Our seasoned professionals shape government policies and foster stakeholder communication, while our think tank explores the political, regulatory, and socioeconomic landscape of the MEA region to drive positive societal change. Focused on Egypt and the MEA region, IPA provides strategic guidance to navigate the evolving business environment, ensuring success through informed decision-making.

CONTACT US

(+2) 25213210/1

ipa@influence-me.com

www.ipa-mea.com