



Executive Regulations of the Personal Data Protection Law

Assessing the Translation of General Rules into
Enforceable Obligations

(Legal Commentary by Masaar – Technology & Law Community,
and the Egyptian Initiative for Personal Rights)

Executive Regulations of the Personal Data Protection Law:

Assessing the Translation of General Rules into Enforceable Obligations

(Legal Commentary by Masaar – Technology & Law Community, and the Egyptian Initiative for Personal Rights)

Arabic Edition: February 2026

English Edition: July 2026



All printing and publication rights reserved. This report may be redistributed with attribution for non-profit purposes under Creative Commons license.

www.creativecommons.org/licenses/by-nc/3.0

Massar is a group of lawyers and technologists interested in enhancing and promoting digital rights and related freedoms in Egypt. We focus on merging law and technology and deepening our understanding of their impact on individuals, society and fundamental freedoms. Our community aims to provide the legal and technical expertise needed by society and individuals to meet challenges pertaining to digital surveillance, privacy, freedom of information, freedom of expression, censorship and digital media.

To contact Massar: masaarnet@gmail.com

The Egyptian Initiative for Personal Rights (EIPR) has been working since 2002 to strengthen and protect basic rights and freedoms in Egypt, through research, advocacy and litigation in the fields of civil liberties, economic and social rights, and criminal justice.

For more information see <https://eipr.org/en>

Background

On July 15, 2020, the Personal Data Protection Law No. 151 of 2020 was promulgated as the first Egyptian regulatory framework establishing rules governing the processing of personal data, partially or fully, electronically. The Law entered into force three months following its publication, thereby becoming effective in October 2020. The legislator further mandated that the Minister of Communications and Information Technology issue the Executive Regulations within six months of the Law's entry into force.

The Law has been drafted by breaking down a significant number of rules and obligations into broad general provisions, the details, procedures, and technical standards of which are to be determined by the Executive Regulations. Consequently, it was hardly possible to immediately implement many of the regulatory provisions, since their practical application necessarily requires specific procedural and technical standards that can be relied upon for assessment, verification of compliance, and the establishment of legal liability in the event of a violation.

This legislative design exclusively placed the regulation of a quite significant set of rules in the hands of the executive authority -represented by the Ministry of Communications- thereby making it the primary controller of how the law is applied and how many of its provisions are interpreted. As a result, the law has lost considerable regulatory autonomy and its capacity for direct application, independent of later referencing or commentary on the regulatory rules and decisions issued by the executive authority through the Executive Regulations.

The impact of this legislative choice was evident in the topics delegated to the Executive Regulations. These Executive Regulations were entrusted with elaborating the details of several pivotal files, foremost among them: regulating the system of licensing, authorization, and accreditation for data collection and processing activities; determining the categories of such licenses, as well as the procedures for their issuance, renewal, and associated fees; in addition to establishing the technical standards and procedural rules for securing data within Egypt and in cross-border contexts. The Regulations also address the registration and delineation of the data protection officers' responsibilities.

Such delegations further extended to matters affecting enforcement and evidentiary standards, such as the determination of the conditions governing the probative value of digital evidence derived from personal data. They further encompass the controls, standards, and precautionary procedures relating to crossborder data transfers, as well as the necessary safeguards for making such data available to a controller or processor located outside the country.

The delayed issuance of the Executive Regulations has disrupted a substantial portion of the Law's operational framework and postponed its transition from a general legislative framework to enforceable rules capable of practical application and accountability. The preparatory process for these Regulations remained unclear regarding its stages, timeline, and consultation mechanisms until they were officially promulgated on the 1st of November 2025 by virtue of the Minister of Communications and Information Technology Decree No. 816 of 2025, issuing the Executive Regulations of the Personal Data Protection Law.

Introduction

This paper serves as a legal commentary and analysis of the Executive Regulations of the Personal Data Protection Law, on the premise that the issuance of the Regulations effectively determines the detailed rules governing the lifecycle of personal data within both public and private entities; the manner in which data subjects exercise their rights; the scope of obligations imposed on controllers and processors; and the oversight and enforcement mechanisms available to the state.

Consequently, a thorough analytical reading of the Executive Regulations becomes essential to ascertain what has been added to the legislative framework, what has been redefined, narrowed, or expanded at the level of application, and the potential direct implications of such changes for the right to privacy and the protection of personal data.

The paper adopts an approach that examines the Executive Regulations as an operational instrument of the Law, insofar as they translate general rules into measurable and enforceable procedures, standards, and institutional roles. Within this framework, the paper assesses the Regulations from two perspectives:

- The first is a legal-procedural perspective, which concerns the clarity and enforceability of the rules, and the extent to which they define the responsibilities of the relevant parties in a manner that prevents ambiguity and limits arbitrariness.
- The second is a human-rights perspective, which concerns the adequacy and proportionality of the restrictions and procedures in relation to the Law's protective purpose, and whether the Regulations strengthen the safeguards available to data subjects or impose additional burdens or administrative pathways that may undermine the effective exercise of rights.

The paper also considers the impact of the discretionary powers granted by the Regulations to regulatory authorities, as well as the extent to which procedural safeguards for licensing, supervision, inspection, and complaint handling are robust, adequately structured, and secure.

Accordingly, the paper is structured along two main tracks. The first examines the extent to which the Executive Regulations fulfill the requirements of the delegation assigned to them by the Law, by tracing the matters whose details were left by the Law to the Regulations, outlining how they were addressed, and assessing whether such a regulation is sufficient to ensure consistent, enforceable, and accountable application.

The second track focuses on identifying the significant issues revealed by the Executive Regulations at the levels of regulatory design, rights protection, and compliance feasibility, and on analyzing their practical impact on data subjects and on entities subject to the Law's provisions. The paper concludes with a set of observations and recommendations aimed at supporting the consistency of the data protection framework with the constitutional and rightsbased objectives of safeguarding privacy, while enhancing the enforceability of the Law without undermining fundamental rights guarantees.

The issues highlighted in this paper reveal that, despite the Executive Regulations addressing a significant portion of the legislative mandates set out in the Law, they continue to generate a degree of legal uncertainty. This uncertainty appears both in relation to implementation timelines, including the

overlap between the date of issuance, publication, entry into force, and the deadlines for compliance and regularization, and in relation to the application of the Law itself.

At the same time, the Regulations deepen concerns over the erosion of meaningful explicit consent (the consent of the data subject). In practice, they treat the mere provision of personal data for the purpose of obtaining a service as constituting implied consent, without establishing binding minimum standards for notice and informed understanding, or safeguards preventing the excessive collection of unnecessary data.

The Regulations also fail to clearly determine the cost of exercising rights or the criteria for their assessment, leaving such matters to subsequent decisions. Nor have they established a unified procedural framework for requests for access, rectification, erasure, withdrawal of consent, and objection (including the recipient entity/authority, the form of the request, the consequences of nonresponse, time limits, and the measurement mechanism): this gap, thereby, risks fragmenting rights into inconsistent pathways across entities and undermining measurability and accountability.

Broader problems also emerge, risking the comprehensiveness of data protection and the governance of law enforcement. The broad exemptions, particularly the national security exceptions, with their loose wording and unconstrained binding powers, as well as the exemptions granted to the Central Bank and the banking sector, deepen the risk of fragmented levels of protection, uneven rights, and enforcement mechanisms depending on the entity controlling the data, thereby affecting the very essence of the principle of comprehensiveness.

On the other hand, the Regulations impose stringent restrictions on cross-border data transfers by requiring prior licensing/authorization even where an adequate level of protection exists. At the same time, the operation of the exceptions still requires more specific controls.

In addition, the absence of a binding framework for annual reporting and the publication of aggregated data, as well as the weak regulation of awareness-raising and training functions, undermines public trust and increases the risk of selectivity or arbitrariness in the enforcement of a highly sensitive regulatory regime.

First: The Extent to Which the Executive Regulations Fulfill the Delegated Requirements under the Personal Data Protection Law

The Law has set out a substantial number of rules and procedures, delegating their detailed regulation to the Executive Regulations. A comparative reading of the provisions of the Law and the Regulations indicates that the Executive Regulations, in general, have addressed most of the detailed matters referred to for regulation.

However, this fulfillment remains closer to a formal compliance with legislative delegations than to the establishment of robust operational rules capable of enhancing legal certainty. The following section outlines the main subject areas and the manner in which the Regulations address them:

1. General Framework for Data Collection and Processing and the Obligations of the Controller and Processor

Article (3) of the Law requires the Executive Regulations to define the standards and controls governing the collection, processing, storage, and security of personal data. The Regulations address this requirement in Article (2) by establishing a general framework governing data processing operations from the moment of collection until retention.

In this context, the Regulations require the data subject's consent before the collection of personal data, along with a clear notification of the purpose of processing. The Regulations consider that the provision of data by the data subject for the purpose of obtaining a legitimate service constitutes implied consent to the processing necessary for that service, while prohibiting the use of the data for another purpose without obtaining new consent. The Regulations also require that the retention period be determined in accordance with the purpose for which the data was collected, and impose obligations to maintain confidentiality, and to prohibit the circulation or disclosure of data except within the limits permitted by law.

Article (4) of the Law further establishes specific obligations on the controller as the entity responsible for the collection of personal data, while delegating the policies, procedures, and technical standards governing these obligations to the Executive Regulations. The Regulations address this delegation in Article (3) by detailing the controller's obligations, including obtaining a license or permit from the competent Center before processing data; not deviating from the specified purpose of processing; verifying the accuracy of personal data from its source before use; erasing data upon the expiry of the specified purpose and notifying the data subject thereof; refraining from retaining data in a form that permits identification of the data subject after the purpose has ended; and correcting any inaccuracies in the data immediately upon becoming aware of them.

Article (5) of the Law delegates to the Executive Regulations the task of determining the detailed policies, procedures, and standards governing the obligations of the data processor, i.e., the entity that processes data on behalf of others. Accordingly, Article (4) of the Regulations sets out detailed safe-

guards that substantially intersect with the obligations imposed on the controller, while taking into account the nature of the processor's role as an executor of processing operations carried out for or on behalf of a controller.

The Regulations require obtaining a license or permit from the Data Protection Center before commencing the activity, and mandate the establishment of an approved mechanism for determining the volume of data and the purpose of processing, as well as documenting the data subject's consent and the extent to which they have been informed of the processing period. They further oblige personnel to maintain the confidentiality of data and refrain from disclosing it, while granting inspectors from the Data Protection Center the authority to oversee and verify compliance with data security and protection measures.

For foreign controllers and processors without an established branch in Egypt, the Regulations impose a specific obligation to appoint a local representative and obtain accreditation from the Data Protection Center. Article (4) also prohibits processing data for purposes other than those specified by the controller, except for statistical or educational purposes conducted on a non-profit basis, and subject to clear conditions, namely the data subject's consent, the relevance of the study to the data, and the anonymization or coding of data in a manner that prevents the identification of data subjects.

2. Use of Data in AI Training & Emerging Technologies

The Executive Regulations explicitly address the use of data in the training of artificial intelligence (AI) systems and emerging and innovative technologies. Clause (7) of Article (4) of the Regulations stipulates that the processor shall ensure such use is conducted "in accordance with the principles commonly recognized at the local, regional, and international levels", and to the extent necessary to ensure that these technologies are employed in a manner that does not result in any harm to the data subject.

This text implies that the Regulations treat the training of AI models as a form of data processing that requires additional considerations, given the nature and expansive impact of such technologies, as well as the potential consequences of their outputs in classification, prediction, and data-driven decision-making.

This means that, where AI systems are trained on data protected under the Law, the processor must carry out such processing in accordance with established professional standards and widely recognized data protection principles. This includes—at a general level—adherence to the specified purpose and not exceeding its scope; data minimization to the extent necessary for training; the adoption of adequate technical and organizational measures to secure the data and prevent its misuse; and ensuring an appropriate degree of transparency regarding the nature and limits of such use, where required within the context of the relationship with the data subject.

In addition, due regard must be given to safeguards that prevent adverse effects on the data subject, whether in the form of direct harm resulting from data disclosure or breaches, or indirect harm arising from the use of training outputs in contexts that affect individuals' rights or legitimate interests.

The provision also requires processors to avoid causing harm, meaning that the use of personal data in AI training must be designed and managed in a precautionary manner that minimizes risks to data subjects. The processor is therefore required to adopt measures and tools that prevent outcomes which could infringe upon individuals' rights or expose them to harm, as part of their professional and legal obligations when using emerging technologies in the context of personal data processing.

3. Notification of Data Breaches and Violations

Article (7) of the Personal Data Protection Law obliges the controller and the processor to notify the Data Protection Center of any breach or violation within 72 hours of becoming aware of it, and to inform the data subject within three working days, while delegating the detailed procedures to the Executive Regulations.

Article (5) of the Regulations establishes a more detailed procedural framework, requiring the creation of a secure electronic register in which all data breaches are recorded, in a manner that enables proper documentation and follow-up. This log must include: the timing of becoming aware of the breach and the timing of notification; the nature and causes of the breach; the volume of data affected; its potential impacts or consequences; the corrective measures taken; the contact details of the data protection officer of the entity; and any additional information requested by the Center.

The Regulations also reiterate a particularly sensitive requirement: the obligation to notify the Center immediately when the breach implicates national security, along with the submission of additional information concerning the nature of that connection.

As for notifying the data subject, the Regulations reaffirm the obligation to do so within three working days from the date of notifying the Center, while specifying that notification must be made through a pre-agreed method (such as SMS, email, or telephone communication).

4. Data Protection Officers Registration and Accreditation: Their Functions and Obligations

Article (8) of the Law requires the establishment of a register at the Center for the registration of Data Protection Officers, and delegates to the Executive Regulations the specification of the conditions, procedures, and mechanisms for such registration. This requirement reflects the recognition that a qualified and accredited Data Protection Officer is a key pillar of compliance for entities that collect or process data.

The Regulations address this matter in Articles (7), (8), and (9), setting out the conditions for the registration of a Data Protection Officer. These include possession of relevant academic qualifications or professional certifications, coupled with relevant practical experience; successful passing of examinations accredited by the Center; and good reputation, including the absence of convictions for offenses involving dishonor or breach of trust.

The Regulations also specify the documents required for registration, including a copy of the national identity card, a recent personal photograph, details of academic qualifications, years of professional experience, a criminal record certificate, proof of passing the required examination, and any previous registration code in case the person has been previously registered.

The Regulations further set out the procedures for reviewing registration applications and issuing decisions thereon within thirty working days from the date of submission, with the Center empowered to request the completion of any missing documents within a specified period. A decision must then be issued within fifteen days from the date of completion. The Regulations also require that each entity's legal representative register its Data Protection Officers so that they may perform their duties in accordance with the provisions of the Law.

Article (9) of the Regulations establishes an electronic register at the Center for the registration of Data Protection Officers, assigning each officer a unique identification code indicating the volume and nature of the data they are authorized to handle, based on the outcome of their examination. Registration applications may be submitted electronically, either by the controller or processor on behalf of an employee, or by the individual themselves seeking accreditation, thereby establishing a clear framework for the qualification, certification, and documentation of the scope of competence of Data Protection Officers.

In connection with this procedural framework governing the registration and accreditation of Data Protection Officers, Article (9) of the Law sets out the core role and primary responsibilities of the Data Protection Officer, while delegating to the Executive Regulations the determination of any additional obligations, procedures, and functions. Accordingly, Article (12) of the Regulations introduces a set of detailed obligations that supplement the role established under the Law and operationalize it within entities subject to its provisions.

The Regulations require the Data Protection Officer to monitor the implementation of the Center's security policies within the controller or processor, and to prepare an annual report to be submitted to the Center on the state of privacy protection. They further provide that, in the event of a change in the Data Protection Officer, the successor shall submit a report to the Center within fifteen days detailing the status of privacy protection within the entity.

The Regulations also oblige the Data Protection Officer to follow up on the receipt of complaints and requests submitted by data subjects, ensure their proper handling, and carry out their functions in a manner that does not conflict with any other assignments that may compromise data protection. They further require the establishment of a separate operational framework in which a single officer serves multiple entities to avoid breaches or conflicts of interest.

These obligations are in addition to the duties set out in the Law, including conducting periodic assessments of security systems, acting as a point of contact with the Center, facilitating the exercise of data subjects' rights, and reporting breaches, among others. Collectively, these responsibilities position the Data Protection Officer as a central link between, on the one hand, internal compliance requirements within the entity and the rights of data subjects, and, on the other hand, the regulatory oversight exercised by the Center.

5. Digital Evidence Probative Value: Personal Data and Criteria

Article (11) of the Personal Data Protection Law stipulates that digital evidence derived from personal data shall have the same probative value as evidence derived from written data and information, provided that such evidentiary value is contingent upon compliance with technical standards and conditions to be specified by the Executive Regulations.

Pursuant to this, Article (13) of the Regulations elaborates the standards governing digital evidence by requiring that the collection or extraction of such evidence be carried out using techniques that ensure the data is not altered, updated, erased, or distorted. It further requires that the evidence be relevant to the incident in question and fall within the scope of the matter to be proven or refuted, in accordance with the decision of the competent investigative authority or court.

Article (13) of the Regulations has also set out the scope of work of the competent authority responsible for the collection, extraction, and preservation of digital evidence, limiting such functions to judicial officers vested with investigative powers or to specialized experts affiliated with investigative or judicial bodies. It further requires that the specifications of the software, tools, and devices used be documented in official records or technical reports, in a manner that ensures the integrity of the original evidence and protects it from tampering.

The Regulations further introduce a procedural requirement for documenting digital evidence before examination and analysis, through an official record prepared by the competent authority. This includes producing printed copies of the media on which the evidence is stored or capturing it through visual or digital means and certifying such copies, while recording the date and time of printing or capture, the identity of the person carrying out the process, the details of the devices, equipment, and tools used, and the data and information relating to the content of the seized evidence. This establishes a comprehensive technical and procedural framework for conferring the evidentiary value referred to in Article (11) of the Law. However, the article does not provide a clear definition of the competent expert bodies or the criteria for selecting them.

6. Controls of Sensitive Personal Data and Children's Data

Article (12) of the Personal Data Protection Law establishes a special regime governing the handling of sensitive personal data, grounded in a general prohibition. Accordingly, controllers and processors—whether natural or legal persons—are prohibited from collecting, transferring, storing, retaining, processing, or making such data available without first obtaining a license from the Data Protection Center.

Except in cases expressly permitted by law, the same Article mandates obtaining the data subject's explicit written consent. It further stipulates that any processing concerning children's data must be subject to the consent of a legal guardian, with a specific safeguard that a child's participation in a game, competition, or any other activity must not be conditioned on the provision of data exceeding what is necessary for such participation. Article (12) of the Law also delegates to the Executive Regulations the task of establishing the standards and safeguards governing this category of data and determining the means of its protection.

Based on the foregoing, Article (14) of the Executive Regulations sets out the standards and safeguards that controllers and processors must observe when handling sensitive personal data. It establishes, as a primary requirement, the obligation to obtain a license or permit from the Center in accordance with the nature of the activity and the categories of licenses and permits specified in the Regulations. It further conditions this requirement to the obtaining of explicit written consent—whether in paper or electronic form—from the data subject, or from the legal guardian in the case of children’s data, except in cases expressly permitted by law.

The Regulations further provide that the collection and processing of such data must be limited to what is essential and necessary for the purpose related to the nature of the controller’s or processor’s activities, in a manner that ensures that no harm results to the data subject. They also require compliance with the Center’s security standards when handling this category of data.

The Regulations also impose additional safeguards governing children’s participation in games, competitions, and similar activities. They prohibit the collection of any data from children beyond what is strictly necessary for participation, and ban the use of such data for profiling, tracking, or behavioral monitoring of children. They further authorize the Center to adopt additional standards, as approved by its Board of Directors, to strengthen the protection of sensitive personal data.

In addition, Article (14) of the Regulations requires the controller or processor to maintain secure electronic records in accordance with the Center’s requirements, ensuring that the handling of sensitive personal data is documented in a manner that allows for traceability and oversight. Such records include, in particular, the recording of the consent of the data subject or the child’s legal guardian when processing sensitive data in any of the forms specified, as well as the recording of requests for deletion, erasure, rectification, or suspension of processing submitted by the data subject or the child’s guardian, together with evidence that such requests have been acted upon.

This framework is further reinforced by Article (15) of the Regulations, which sets out specific safeguards governing children’s data. The provision regulates the process for obtaining parental or guardian consent before collecting or processing the personal data of children under 15, whether for the purpose of providing a service or for any other purpose. The Regulations also require that such consent specify its period of validity, without prejudice to the parent or guardian’s right to withdraw or modify that consent at any time. In addition, the authority to approve the mechanisms and formats for issuing these consents is vested in the Center.

The same Article also addresses the age group of 15 to 18 years, requiring either the child or their parent or guardian to provide consent for the collection and processing of the child’s personal data. The Regulations further assign the Center responsibility for determining the mechanisms governing this process to ensure compliance with applicable legal requirements.

7. Personal Data Cross-Borders: Controls of Transfer and Disclosure

Article (14) of the Law prohibits the transfer, storage, processing, or disclosure of personal data outside Egypt unless an adequate level of protection—no less than that prescribed under the Law—is

ensured, and subject to obtaining a license or permit from the Data Protection Center. It further delegates to the Executive Regulations the establishment of the policies, standards, and safeguards governing such activities.

Article (16) of the Regulations extensively addresses this issue, establishing a framework based on a set of layered constraints governing cross-border data transfers. Foremost among these is the requirement to obtain prior authorization—by way of a license or permit from the Center—for transferring data to a foreign country. Granting such authorization is contingent upon an assessment of the adequacy of the protection in the receiving country, as well as the data subject’s consent to the transfer of their data.

The regulations further impose technical and organizational obligations to protect data during transfer, circulation, or storage abroad. They restrict transfers to the countries specified in the license and require that the license be updated when new countries are added, thereby defining and constraining the scope of transfer within the limits of the license itself, in terms of both destination countries and the presumed safeguards for data protection.

The framework established by the Executive Regulations reflects that the transfer of personal data across borders is managed through an approach based on prior licensing or authorization as the primary gateway for permitting transfers, in which the decision to transfer is initially contingent on an authorization issued by the competent authority. Pre-authorization thus becomes the central mechanism for regulating cross-border data flows, with the consequence that the scope of transfers is confined to the countries approved under the license and is subject to mandatory updates when additional countries are to be included.

In the context of cross-border data transfer regulation, Article (16) of the Law permits the controller or processor to share personal data with a party outside Egypt, subject to authorization from the Center, provided specific conditions are met. These conditions include the alignment in the nature of activities or purpose between the parties, the existence of a legitimate interest, and the assurance of a level of protection not less than that prescribed in Egypt. The Law delegates to the Executive Regulations the establishment of the necessary conditions and precautions in this regard.

Article (17) of the Regulations further elaborates the conditions governing the disclosure of personal data across borders. It requires that the activities and services of both parties be aligned or complementary in a manner that serves a legitimate interest of either party or the data subject. It also mandates the adoption of safeguards that ensure, at the recipient’s end, a level of legal and technical protection for the data that is not less than that applicable in Egypt, in addition to any further safeguards or standards prescribed by the Center.

Accordingly, “disclosure” to a foreign party is framed as a parallel regulatory regime to cross-border transfers, grounded in authorization, conditions, and safeguards, with its lawfulness contingent upon the existence of a legitimate interest and the assurance of an equivalent level of protection in the receiving jurisdiction.

8. Direct Electronic Marketing: Governing Regulations

Articles (17) and (18) of the Personal Data Protection Law set out the conditions and safeguards governing direct electronic marketing, including the requirement to obtain the data subject's consent, to identify the sender clearly, and to provide an accessible means to object or unsubscribe. Article (18) further delegates to the Executive Regulations the establishment of the detailed rules, conditions, and safeguards applicable to this type of processing.

On this basis, Article (18) of the Regulations addresses direct electronic marketing, distinguishing between pre-activity obligations imposed on the sender—applicable to any electronic communication for direct marketing—and the safeguards governing the manner in which such marketing is conducted.

Regarding the conditions incumbent upon the sender, whether a controller, processor, or marketing intermediary, the Regulations require obtaining a license from the Center to carry out electronic marketing activities, securing the data subject's prior explicit consent before sending marketing communications, and erasing the personal data of the targeted individual where consent is withdrawn or where the purpose or the specified duration of processing has expired.

As for the safeguards governing the conduct of marketing activities, the Regulations prohibit the use of data collected for marketing purposes for any other purpose, or its disclosure to third parties without renewed consent. They also require that each message or communication clearly identify, from the outset, the sender and its marketing purpose, while the data subject be easily able to refuse further communications or unsubscribe through a mechanism approved by the Center, whether via SMS, email, telephone, or other means.

The regulatory framework also extends to marketing intermediaries, requiring them to verify that the originating entity has obtained the data subjects' consent before using their data, and to maintain records evidencing the source of the data, proof of consent, and any objection requests received.

The Regulations further require the sender to maintain electronic records, accessible to the Center upon request, documenting the manner and date of obtaining the data subject's consent, any requests for withdrawal or modification of consent, and the measures taken in response to such requests, as well as the security mechanisms implemented during the marketing campaign. They also designate a dedicated channel at the Center for receiving public complaints related to direct marketing communications.

9. Licenses, Authorizations, Data Protection Accreditations, and Their Fees

The Executive Regulations establish the framework governing licenses, authorizations, and accreditation certificates as fundamental regulatory tools for implementing the provisions of the Personal Data Protection Law. This includes defining the relevant categories and tiers, setting the conditions, procedures, application forms, issuance and renewal mechanisms, and regulating fees within the ceilings prescribed by the Law, namely not exceeding EGP 2,000,000 for a license and not exceeding EGP 500,000 for a permit or accreditation.

Within this framework, Article (19) of the regulations establishes a classification of licenses for legal persons according to the volume of personal data records held by the controller or processor. This begins with an exemption from fees for the smallest category, and then increases progressively as the volume of data grows, up to the prescribed maximum for those whose records exceed five million.

In addition to the criterion of data volume, the Regulations distinguish between a license covering both the controller's and processor's activities and a license limited to either function. Accordingly, fees are reduced by 50 percent where the activity is restricted to a single role. The Regulations also introduce reduced fixed fees for certain categories, including civil society organizations, trade unions, and clubs.

Concerning authorizations, Article (20) of the regulations establishes a framework for temporary authorizations lasting less than one year, linking the fee to two factors: the duration of the authorization and the volume of data being processed. The fee structure follows a progressive scale, starting with exemptions for smaller categories and reaching the statutory maximum for larger ones, while replicating the 50 percent reduction where the permit is limited to either the controller's or the processor's activity alone.

In parallel with the regulation of licenses and authorizations, the Regulations also organize accreditation certificates for consultants working in the field of data protection, as a mechanism for accrediting consultancy providers, whether natural persons (e.g., individual experts) or legal persons (e.g., consultancy firms). Articles (32) and (33) set out the conditions for obtaining an accreditation certificate to provide data protection consultancy services, requiring, in the case of individual consultants, relevant academic qualifications or professional certifications together with practical experience, and, in the case of legal persons, evidence of the entity's activity and expertise in the field.

Article (34) sets the fee for the accreditation certificate at EGP 5,000 per annum, stipulating a validity period of three years, renewable upon payment of the same fee. This establishes a procedural and fee-based framework for accrediting consultancy service providers within the compliance system operationalized by the Executive Regulations.

Second: Key Issues in the Executive Regulations

Although the Executive Regulations cover a wide range of matters delegated to them under the Personal Data Protection Law, thereby satisfying the Law's formal requirements, several substantive issues emerge upon closer examination. This range spans procedural omissions in respect of certain regulatory rules requiring further elaboration, to incomplete treatment of details that were not fully addressed within the Regulations.

1. Deepening Concerns Regarding the Effectiveness of Explicit Consent for Data Collection and Processing

Obtaining the free and informed consent of the data subject constitutes one of the foundational pillars of privacy and data protection, as it reflects the individual's right to exercise control over their personal data and to determine the limits of its use. The effectiveness of a consent-based regime in any data protection framework is closely linked to the extent to which it is accompanied by safeguards enabling individuals to exercise their rights in practice—such as access, rectification, erasure, and objection—thereby preventing consent from becoming a purely formalistic mechanism used to justify processing without meaningful empowerment of the data subject.

In this context, [Article \(2\)](#) of the Personal Data Protection Law provides that personal data may not be collected or processed except with the explicit consent of the data subject or in cases expressly permitted by law. It further establishes a set of rights for the data subject, including the right to be informed of their data and to obtain it, the right to withdraw consent, the right to rectification, erasure or amendment, the right to restrict or specify processing, the right to be notified of any data breach or violation affecting their data, and the right to object to processing that is contrary to fundamental rights and freedoms.

However, a reading of the Executive Regulations reveals several issues affecting how these rights are operationalized and the extent to which the consent-based regime can, in practice, achieve its protective purpose.

The first of these concerns relates to the formulation of consent and the mechanisms for its verification. [Article \(2\)](#) of the Executive Regulations provides that a natural person's voluntary submission of personal data in the course of a lawful service or transaction shall be deemed consent to its collection and processing for that specific purpose. In practice, this means the Regulations recognize implied consent whenever an individual provides personal data to access a service, such as registering on a website, purchasing a product, or completing a digital transaction.

The problem is not the recognition that a service relationship requires a minimum level of processing to achieve its purpose. Rather, the problem lies in treating the mere provision of data as consent, which may open the door to unrestrained reliance on this logic without ensuring that the individual has adequately understood the scope and limits of the processing. This concern is particularly acute where the principle of purpose limitation and notification is not translated into clearly defined procedural standards.

This approach also creates the possibility of collecting data beyond what is strictly necessary for the provision of the service, particularly as clause (8) of Article (3) of the Regulations leaves the determination of the volume and nature of such data to the law governing the relevant activity. In this context, from both a legislative and a practical perspective, the laws governing most commercial activities, for example, lack specific provisions addressing this issue.

The regulations indeed oblige the controller to clearly notify the data subject of the purpose; however, the provision does not specify the method or its minimum standard. The Regulations fail to clarify whether such notification may be embedded within lengthy privacy policies—which are rarely read by users—or whether it must be provided through a concise and prominent notice at the point of data collection, or through the design of consent interfaces that present the essential elements of processing in simplified language.

Accordingly, the absence of such specification extends its impact to the very essence of informed consent, understood as consent based on a genuine and meaningful understanding, rather than merely the completion of a transaction or the act of clicking a button within general terms and conditions.

In this context, the Regulations could have strengthened the effectiveness of consent by establishing minimum standards for its validity, such as requiring it to be as distinct as possible from general terms, formulated in clear language, and as easy to withdraw as it is to give.

At the very least, they could have provided a framework enabling the issuance of guidance templates or standardized forms to ensure that awareness and understanding are effectively achieved at the time consent is requested, rather than leaving the matter to divergent practices among entities that may strip the requirement of explicit consent of its substance.

2. Data Subject Rights: The Impact of Financial Burden and Procedural Framework

Since its enactment, the Law has sparked debate over its authorization to impose a fee on certain services related to the exercise of rights, including access to data by the data subject, with a ceiling that may reach, according to the Law's authorization, twenty thousand Egyptian pounds. In turn, the Center is entrusted with determining the actual fee for each service within the limits set by the Law.

Although the Executive Regulations were subsequently issued to regulate multiple aspects of compliance, they do not directly address the rules governing the cost of exercising rights, their limits, or the criteria for their assessment. This omission appears to leave these matters to future regulatory decisions to be issued by the Center.

Still, this omission remains a source of rightsbased concern, because the individual's right to know what data entities hold about them, and their right to access, rectify, or erase that data, are not privileges. Rather, they are constituent elements of the right to privacy and data protection itself. Consequently, imposing high financial barriers to exercising these rights creates a de facto disparity in access to justice. It makes individuals' enjoyment of those rights contingent on their ability to pay, which is particularly harmful to lowerincome groups and undermines the Law's protective purpose.

These concerns are further exacerbated by the absence of detailed, binding, and standardized procedures for the exercise of rights; A review of the regulations reveals that some provisions indirectly address scattered aspects of this process. This includes the obligation on the data controller to erase data once the purpose has ceased and to notify the data subject thereof, or the obligation on the data protection officer to follow up on complaints and requests and ensure their implementation, or record-keeping requirements that include evidence of the implementation of requests for deletion, erasure, or modification in certain cases.

The Law affirmed two pathways in Articles (32) and (33): the first is the right of the data subject to submit a request to the data holder/controller/processor concerning the exercise of any of their rights set out in the Law, obliging the latter to respond within six working days. The second relates to lodging a complaint with the Data Protection Center regarding a violation of their rights under the Law, whereby the Center is obliged to respond to the complaint and notify both parties within 30 working days. Importantly, the right to submit a complaint to the Center does not constitute a procedural restriction on the data subject's right to seek a judicial remedy for any violation of their rights.

However, these partial measures do not substitute for the existence of a unified procedural framework that clearly identifies the competent internal unit within each entity for receiving data subjects' requests, whether the Data Protection Officer, a dedicated department, or customer service, and specifies the acceptable form of such requests, including whether a standardized electronic or paper form is required. Such a framework should also establish a fixed timeframe for response, clarify whether failure to respond within that period constitutes a refusal or a procedural default allowing escalation to the Center, and set out a general rule governing the entity's liability for non-implementation or delay.

Leaving such details to each entity's internal practices creates significant disparities in responsiveness. It may, in practical terms, lead to delays or even disregard of individuals' requests, particularly in the absence of a clear mechanism that ensures measurability and accountability.

Among the most significant concerns are the rights to object and to withdraw consent. These are essential safeguards for ensuring that an individual's control over their personal data is not limited to the initial moment of collection, but remains an ongoing form of control that can be exercised later, whether because the processing conflicts with their fundamental rights and freedoms, or because they wish to revoke consent previously given.

Although the Law recognizes the individual's right to object to the processing of their personal data or its outcomes whenever such processing conflicts with their fundamental rights and freedoms, and also affirms the right to withdraw consent for the storage or processing of their data, the Executive Regulations do not establish a general procedural framework governing how such rights are to be exercised.

In particular, they do not clearly specify the actions to be taken by the controller or processor upon receiving an objection, the applicable timeframes for deciding on such requests, the criteria for balancing the entity's interest in continuing processing against the individual's interest in its cessation, or the mechanisms that must be made available to ensure that the exercise of these rights is simple and accessible.

The Regulations do reflect this approach, albeit within a specific context—namely, direct electronic marketing—where they require the provision of accessible mechanisms to refuse communications or

withdraw prior consent. While this represents a positive development, it remains confined to the domain of marketing.

This underscores the need to generalize this approach as a broader principle. Any service or transaction predicated on an individual's consent should ensure the availability of a clear and simplified mechanism for withdrawing that consent or terminating the associated processing, with the same degree of ease as that afforded at the point of granting consent. Such an approach is essential to prevent the right of withdrawal from devolving into a merely theoretical entitlement that is difficult to exercise in practice.

The concerns raised by the Executive Regulations in this context do not pertain to the principle of consent itself, but rather to how it is operationalized in terms of transparency, procedural standards, and the accessibility of rights without prohibitive costs or complex pathways. The effectiveness of an explicit consent regime is not measured solely by the existence of formal provisions, but by individuals' ability to understand what they are consenting to, to exercise their rights with ease, and by the presence of unified procedures against which compliance can be measured and accountability enforced in cases of breach.

3. Broad Exemptions to the Scope of the Law: Derogation from the Principle of Comprehensiveness

At its core, the Personal Data Protection Law seeks to establish a general framework for safeguarding individuals' privacy against potential infringements arising from the collection, processing, and circulation of personal data. However, the scope of application delineated in the Law's promulgation provisions—and subsequently reinforced in certain respects by the Executive Regulations—incorporates broad exemptions that may, in specific sectors, curtail the extent of protection or render it uneven depending on the entity undertaking the processing and the nature of the activity.

Article (3) of the promulgation provisions exempts the application of the Law across six principal domains, including processing for purely personal use; processing undertaken for the purpose of producing official statistics or in implementation of a legal obligation; processing for media purposes, subject to conditions relating to accuracy, integrity, and non-use beyond journalistic purposes; data related to judicial policing, investigations, and litigation; data held by national security entities (and as determined necessary for national security considerations); and data held by the Central Bank of Egypt and entities under its supervision (except money transfer and exchange companies), while respecting the Central Bank's rules governing data.

The Law further grants national security authorities the power to require the controller or processor to amend, erase, or withhold the display of personal data within a specified timeframe based on national security considerations, with an obligation on the controller to comply immediately.

The core concern is the exemption for national security authorities, both in its breadth and the additional powers it entails. The formulation referring to national security entities and "what they deem necessary for national security considerations" opens the door to broad interpretation regarding the

scope of entities covered and the criteria for invoking the exemption. Moreover, in terms of its effect, it confers discretionary authority on such entities to request the amendment, erasure, or suppression of personal data held by other entities, and imposes an obligation on the controller or processor to implement such requests immediately.

The difficulty lies in the fact that the notion of national security is articulated in broad and open-ended terms, without objective or procedural delineation of its limits or conditions of application. This weakens the foreseeability of the exemption's use and renders its scope susceptible to expansion based on administrative discretion.

While Clause (5) of Article (3) of the promulgation provisions of the Personal Data Protection Law empowers national security authorities to notify the controller or processor to amend, erase, suppress, or restrict the display, availability, or circulation of personal data, it does not establish substantive limitations on the types of data concerned or the circumstances justifying such requests. Nor does it clarify whether effective oversight mechanisms exist to regulate the exercise of these powers—whether judicial, parliamentary, or independent oversight. This raises the risk that the exemption may, in practice, evolve into a sphere beyond the protection of the Law, one that is not governed by standards of legal certainty and does not permit clear accountability regarding the grounds and limits of such interventions.

Protecting national security considerations may indeed be invoked in certain contexts as a legitimate interest. However, from a constitutional and human-rights perspective, introducing such a broad exemption requires that the restrictions be specific, clear, and controllable. They also require safeguards to avoid becoming a gateway to sweeping exemptions or to binding orders ungoverned by criteria.

As for the exemption concerning the Central Bank of Egypt and its affiliated entities, the problem is no less significant, as it excludes the banking sector from the Law's scope, relying instead solely on the Central Bank's own rules for protecting customer data.

Although sector-specific regulations may provide some protection, the blanket exemption directly affects data subjects' rights and the mechanisms for enforcing them. Rights such as withdrawing consent, objecting to processing, or lodging complaints with the Data Protection Center may not apply when dealing with an entity excluded from the scope of the Law, thereby confining the scope of protection and oversight to the sector-specific framework itself rather than to the general system established by the Law.

This results in a duality of protection levels and a disparity in the safeguards available to individuals, depending on the entity holding their data. Such disparity is particularly pronounced in financial data, which, by its nature, constitutes one of the most sensitive categories of personal data, with significant implications for individuals' personal and economic security.

This exemption also raises questions about whether it is necessary in its entirety. In principle, it could have been possible to address any potential conflict of jurisdiction or regulation through clear coordination mechanisms between the sectoral authority (such as the Central Bank) and the general authority established under the Law (the Data Protection Center). Such an approach could have preserved the Law's applicability, along with the rights, safeguards, and enforcement mechanisms it provides, rather than excluding an entire category of transactions and data from its scope.

4. Cross-Border Data Transfer: Concerns Regarding Restrictions and Exemptions

The transfer of personal data across borders is one of the most sensitive issues in international data protection, as it lies at the intersection of the protection of privacy on the one hand and the demands of a globalized digital economy and the operation of cross-border services on the other.

In this context, modern legislative approaches tend to permit data flows on the condition that an adequate level of protection is ensured in the receiving country, rather than adopting strict prohibitions or regulatory closure that may negatively impact the digital services environment. By contrast, the Egyptian Law adopts an approach that prohibits the transfer of personal data outside Egypt unless a license or permit is obtained from the Data Protection Center, and the adequacy of the level of protection in the foreign jurisdiction is verified.

The Executive Regulations attempt to provide a more detailed framework for this approach by establishing assessment criteria and envisaging the adoption of a list of countries deemed to provide an adequate level of protection. Nevertheless, practical concerns remain, as the regulatory structure itself imposes a fundamental burden: prior authorization is an inherent condition for transfer. Even where the receiving country ensures a level of protection equal to or higher than that in Egypt, a license or permit must, in principle, still be obtained from the Center. Moreover, the scope of the authorization is strictly limited to the countries expressly specified therein, requiring further updates whenever an additional country is to be included.

In parallel with the prior authorization regime established by the Regulations, the Law itself retains a significant set of exceptions permitting the transfer of personal data to countries that do not provide an adequate level of protection. Pursuant to [Article \(15\)](#), such transfers are allowed in specific cases, including where the data subject has given explicit consent; where necessary to protect the life of the individual or to provide medical care; for the performance of legal obligations or enforcement of judicial decisions or judicial cooperation; for reasons of public interest; in the context of monetary transfers in accordance with the laws of the receiving country; or in implementation of international agreements.

As a matter of principle, such exceptions are not uncommon in data protection regimes, as they typically provide mechanisms that allow cross-border transfers in narrowly defined circumstances to avoid obstructing essential interests or legal obligations that cannot be fulfilled without them. However, the practical concern here is how these exceptions are operationalized and the limits of their interpretation, particularly when they are not accompanied by clear procedural safeguards that specify the conditions, scope, and criteria for necessity and proportionality applicable to each exception.

Certain formulations—such as “necessity for the protection of the public interest”—are inherently broad and may be invoked to justify data transfers without sufficient constraints if not anchored in precise, assessable standards. This, in turn, may open the door to divergent interpretations across entities, undermining legal certainty and affecting data subjects’ ability to anticipate how their data will be handled in cross-border contexts.

5. Data Protection Center: Broad Authority and Full Subordination

The Personal Data Protection Law establishes the Data Protection Center as a public economic authority affiliated with the Minister of Communications and Information Technology and entrusts it with a wide range of powers, positioning it at the core of the data protection framework and as the primary authority responsible for its operation.

The Center is competent to issue licenses, permits, and approvals required for processing activities; accredit Data Protection Officers and consultants; receive and adjudicate complaints and issue decisions thereon; carry out inspection and supervisory functions; develop policies, rules, and safeguards related to data protection; and coordinate with governmental and non-governmental entities, among other regulatory and executive functions.

This institutional design effectively concentrates regulatory, supervisory, and enforcement powers within a single authority. Such concentration is directly linked to two interrelated considerations: first, the degree of the Center's independence from direct governmental influence; and second, the transparency of its operations and its capacity to engage stakeholders in developing its policies and standards.

At the level of institutional independence, the Law does not treat the Center as a fully autonomous body; rather, it embeds it within an executive structure affiliated with the competent minister, reflecting the governance model adopted by the legislature. The Law does not establish full independence for the Center, insulating it from executive influence or potential conflicts of interest when regulating sectors that intersect with ministerial competencies. Instead, it places the minister in a central position within the decision-making structure, as the minister chairs the Center's Board of Directors. Moreover, the composition of the Board includes representatives from various governmental and security-related entities, further reinforcing its administrative integration within the executive framework.

This model raises practical questions regarding the Center's capacity to regulate entities in which the State—or the minister, being the chairman of the Board—may have a direct or indirect interest in their activities. This concern is particularly salient in sectors that are among the largest collectors and processors of personal data and the most influential in data governance, including governmental bodies and major companies operating in telecommunications or in the provision of digital public services.

Moreover, the lack of sufficient independence undermines public trust in the Center's decisions and impartiality, making it more vulnerable to political or economic influences by virtue of its subordination and the dominance of representatives of governmental bodies in its board structure. Although this issue is primarily rooted in the design of the Law itself rather than in the Executive Regulations, it remains relevant to the overall assessment of the regulatory framework's effectiveness.

Issues of transparency and participation emerge as a parallel condition for sound governance and the legitimacy of regulatory rule-making. From the moment of the Law's enactment—and subsequently during the drafting process of the Executive Regulations—concerns were raised regarding the limited transparency of the drafting process and the scope of public consultation, as well as the extent to which deliberative channels were sufficiently open to allow for an adequate assessment of the breadth and balance of stakeholder participation.

With the Center entering its operational phase, its institutional responsibility becomes correspondingly more significant in establishing regular and publicly accessible channels of engagement with all relevant

stakeholders, ensuring transparency in its policies, decisions, and guidance, and involving the technical, legal, and professional communities, as well as experts, user representatives, researchers, and rights and freedoms stakeholders, in the development of guidelines, codes of conduct, and technical standards that will underpin compliance. The continued operation of the Center as a closed bureaucratic body—even with expanded powers—risks weakening the social acceptance of its decisions and undermining confidence in the fairness of enforcement, thereby rendering compliance less a product of a trusted regulatory system grounded in legal certainty and public confidence, and more a form of externally imposed obligation.

A further implication extends beyond institutional design to the manner in which the Center's broad powers may affect rights and freedoms in practice. The Center is endowed with a range of supervisory and enforcement tools, including inspection powers, judicial police authority, the imposition of binding data protection measures, and the issuance of administrative fines. These instruments are, in principle, intended to strengthen compliance, protect individuals' rights, and deter violations. However, the concentration of extensive supervisory and executive powers within a single authority, combined with limited safeguards for independence and the presence of multiple governmental and security-related representatives within its governing structure, raises concerns regarding the potential for selective enforcement and the discretionary or arbitrary application of regulatory, supervisory, and enforcement measures.

Accordingly, supervisory scrutiny may become disproportionately focused on smaller or less well-resourced entities, while larger actors may be subject to comparatively less rigorous enforcement. There is also a risk that inspection procedures and the identification of formal compliance violations could be used selectively as a means of exerting pressure on certain entities, including media organizations, non-profit organizations, or small enterprises, rather than being directed toward areas of genuine risk and the most significant sources of impact on data subjects' rights.

6. Absence of the Center's Transparency Obligations and Its Awareness-Raising Framework

The range of concerns becomes broader when turning to what the Executive Regulations omit in regulating key functions of the Center that directly affect the transparency of the system, the measurement of its performance, and the ability of the public, Parliament, researchers, and the media to assess it. In this regard, the annual report on the state of personal data protection in Egypt constitutes one of the Center's most important institutional tools, serving as a mechanism for monitoring and public evaluation that reveals key indicators and trends, enables an understanding of the nature of violations and levels of compliance, and tracks the evolution of the system's overall performance.

Nevertheless, despite the Executive Regulations' detailed elaboration of procedures for licenses, authorizations, registration, inspection, and other procedural aspects, they do not dedicate a regulatory framework clarifying how this report is to be prepared, what its scope is, what its minimum content should be, when it is to be issued, or how it is to be published and made available to the public.

This omission results in direct harm, namely converting the report from an accountable, periodic institutional obligation into an unregulated general promise, thereby weakening the ability to track trends in violations, measure the effectiveness of law enforcement, identify the highest-risk sectors, and expose shortcomings in protection.

The Regulations could have included practical details to make the report a transparent and measurable tool. For example, they could have required that the report be published on the Center's website by a fixed annual deadline and established a standardized structure containing a minimum set of aggregated, non-identifying data. This data could include statistics on complaints and reports, their types and outcomes; aggregated data on data breaches, their causes, and the corrective measures taken; patterns of compliance across different sectors; and a general assessment of the implementation of core data protection principles based on inspection and oversight activities.

The Regulations could also have clarified whether the report may include legislative or regulatory recommendations, whether such recommendations are binding or advisory, and how the Center would follow up on their implementation from year to year. In addition, they could have established an internal or consultative review mechanism to ensure the report's quality and prevent it from becoming a formal narrative that obscures shortcomings rather than revealing them.

Similarly, the Regulations reveal a clear omission regarding the Center's expected awareness-raising and training role, including through conferences, workshops, training and educational programs, and the publication of guidance materials. This function is essential to enabling rights in practice. Data protection cannot be achieved through legal provisions alone; it also depends on individuals' ability to understand and exercise their rights, and on the ability of relevant entities to understand their obligations and implement them correctly at both technical and procedural levels.

However, the Regulations do not establish a framework specifying when and how the Center should perform this role, which groups should be targeted, the minimum activities required, or the tools for measuring impact. This leaves implementation vulnerable to becoming selective, seasonal, or directed only at particular audiences, such as larger entities, while users, small businesses, civil society organizations, the media, and other actors remain the weakest links in the compliance chain.

This omission creates a twofold harmful impact. On the one hand, it exacerbates the imbalance of power among controllers, processors, and data subjects, as rights cannot be effectively exercised without knowledge. At the same time, stronger entities are better positioned to comply formally, leaving individuals with limited tools for accountability. On the other hand, it undermines the quality of technical compliance, as many data breaches stem from training and procedural deficiencies rather than intentional misconduct.

The Regulations could have established a minimum practical framework for this function by requiring the Center to adopt a publicly available annual plan for awareness and training, covering key topics such as individuals' rights, complaint mechanisms, breach notification, sensitive data, and cross-border data transfers. This framework could be complemented by developing user-friendly guidance materials and standardized templates, including model privacy policies, clear consent forms, guidance on withdrawing consent, and procedures for handling access and erasure requests.

In addition, the framework could provide for the design of accredited training programs for Data Protection Officers and personnel involved in processing activities, with accreditation and renewal linked to periodic training hours. It would also be important to ensure that publications and guidance are accessible to the general public in clear, simplified language, rather than remaining confined to technical terminology primarily intended for corporate entities.

Third: Recommendations to Strengthen the Legal and Regulatory Framework for Data Protection

Based on the key concerns identified in the Executive Regulations, a set of practical recommendations can be addressed to both the Egyptian legislator and regulatory authorities, particularly the Data Protection Center. These recommendations aim to address existing shortcomings and improve the feasibility of compliance, without undermining the core rights-based protections that the framework is meant to guarantee.

The recommendations fall under three main areas. The first concerns urgent regulatory measures that the Center can issue as binding decisions, guidance documents, or standardized templates. The second includes medium-term legislative proposals that would require amendments to the Law. The third focuses on regulatory and technical improvements to strengthen practical implementation, transparency, and capacity building.

1. Addressing Gaps in the Executive Regulations through Binding Regulatory Decisions and Guidance Issued by the Data Protection Center

It is recommended that the Data Protection Center take the initiative to establish detailed, standardized procedures for data subjects to exercise their rights, so that the rights recognized under the Law are not left as a general framework whose implementation varies from one entity to another. These procedures should be issued as a regulatory decision or a binding guidance document that sets out the process for requests related to access, obtaining a copy of personal data, rectification, erasure, restriction of processing, objection, and withdrawal of consent.

This framework should identify a clear point of contact within each entity subject to the Law for receiving such requests, whether the Data Protection Officer or a designated customer service unit. Entities should also be required to provide an electronic channel for processing digital activities or services and to adopt a standardized request form that can be used in either paper or electronic format.

A reasonable timeframe should also be set for responding to requests. Failure to respond within that timeframe should have legal consequences and be treated as a violation requiring the Center's intervention and the exercise of its supervisory powers.

In the same context, the Center should require controllers and processors to ensure that withdrawing consent is as easy as giving it. Where consent was provided electronically, withdrawal should be available through a simple and direct mechanism. A short timeframe should also be established for implementing the withdrawal, stopping the processing, or deleting the related data, as applicable. The data subject should then be notified once the measure has been completed, in a manner that enables verification of the action.

The effectiveness of these rights also depends on reducing the financial burden placed on individuals when exercising them. The Center should therefore use its authority to determine fees for services related to the exercise of rights in a way that makes exemption, or a very low nominal fee, the default for routine requests. Financial charges should not become a practical barrier to accessing rights.

A reasonable fee should be permitted only in cases involving manifestly abusive or excessively repeated requests, and even then, it should be limited to covering minimal administrative costs. The Center should also issue a clear standard defining abusive requests and how to handle them, to prevent the exception from becoming the rule.

To address the structural deficiencies associated with the breadth of certain exceptions, it is recommended that the Center issue interpretative decisions and procedural guidance to narrow areas of ambiguity to the greatest extent possible within the existing framework, particularly regarding the media exception and the limits of the national security exemption. With respect to the media exception, it would be advisable for the Center to issue guidance clarifying its scope and boundaries in a manner that prevents it from being construed as a blanket exemption from data protection requirements, while reaffirming the professional obligations that preclude the abusive publication of data or the processing of sensitive data without legitimate justification.

Regarding the national security exemption, it is recommended that a procedural cooperation protocol be established with the competent authorities, specifying the form of requests for the modification, erasure, or nondisclosure of data. These requests should be in writing, reasoned, dated, and subject to a minimum level of documentation within the receiving entity. A secure internal log should be established to document and categorize these requests, thereby limiting practical arbitrariness and facilitating subsequent accountability without disclosing potentially sensitive information.

In the context of transparency and the validity of informed consent, it is recommended that the Personal Data Protection Center issue binding standards governing the formulation of consent requests and notification mechanisms at the point of data collection. These standards should establish a mandatory minimum content for such notices, thereby preventing inconsistent practices across entities. They should also promote a layered notice model, whereby a concise and clear notice is presented at the point of collection, indicating—at a minimum—the purpose of processing, the retention period, the core rights of the data subject, and the mechanism for withdrawing consent, alongside the availability of a more detailed privacy policy for those who wish to access comprehensive information.

The standards should also explicitly prohibit embedding consent within lengthy, incomprehensible texts or vague general terms, and prohibit linking consent to a single, nondivisible condition when multiple purposes exist, thereby safeguarding the essence of free, specific, and informed consent in practice.

These standards may be grounded in well-established international references. The EU General Data Protection Regulation (GDPR) defines consent as freely given, specific, informed, and unambiguous consent, which is neither presumed nor implied. Consent must be explicitly and clearly expressed by the data subject either through a direct statement (such as writing “I agree” or signing a clear form) or through a clear affirmative act indicating choice (such as clicking an “I agree” button or ticking a box that is not prechecked).

The GDPR also adds an important rule to protect people from uninformed consent: if a request for consent is embedded in a document that includes other matters (such as terms of use or a contract), the consent must be presented as a separate, clear, and distinguishable section from the rest of the text, so that the individual can see it, understand it, and specifically agree to it – rather than having it hidden within long paragraphs or general wording. The GDPR further confirms that silence, leaving a consent box unchecked, or failing to take any action does not constitute consent, because consent is not presumed but must be evidenced by a clear affirmative act.

From the perspective of enforceability and oversight, it is recommended to complement the procedural framework for exercising rights by requiring every controller and processor to maintain a secure internal register of data subject requests. This register should record the date and type of each request, a summary of how it was handled, the decision—acceptance or refusal—the reasons for any refusal, and the time taken to respond. Such a register should be subject to inspection, thereby helping to prevent denial or manipulation in the handling of requests and transforming rights into measurable and accountable obligations.

With respect to personal data breaches, it is recommended that the Center develop a standardized breach-notification template specifying the minimum information to include in any report. The Center should also issue guidance on assessing the severity of a breach, determining when notification to the data subject is required, and how such notification should be formulated. This framework would help ensure a reasonable degree of consistency and quality in reporting, while enhancing the Center's ability to process and respond effectively to such incidents. In parallel, it is necessary to establish a procedural standard that reduces ambiguity in classifying a breach as implicating national security by defining the minimum elements of reasoning and documentation that must be satisfied within the reporting entity.

The Center should also adopt, in its regulatory decisions, a risk-based approach to the framework's operation, whereby the intensity of oversight, intervention, and documentation requirements is calibrated to the sensitivity and volume of the data, the nature of the processing, and the level of risk posed to individuals. This would avoid a uniform approach that treats low- and high-risk processing activities in the same way. Such an approach could be reflected in the classification of requests, the prioritization of inspections, and the determination of cases requiring enhanced safeguards, thereby supporting more efficient enforcement and ensuring proportionality.

2. Artificial Intelligence and the Use of Personal Data in Model Training

It is recommended that the Personal Data Protection Center issue a specialized guidance document or code of practice governing the use of personal data in the development and training of AI models and emerging technologies. Such guidance would translate the general obligations set out in the Executive Regulations—such as the principle of non-harm—into concrete operational standards that are verifiable, auditable, and enforceable. At a minimum, the guidance should include clear requirements regarding:

- Define the scope of data used and strictly link it to the declared purpose of training, while prohibiting or restricting any unjustified expansion in data collection or use.
- Specific rules for reusing data in training new models or updating existing ones, along with criteria for assessing the lawfulness and limits of such reuse.
- Standards for disclosure and notification when personal data are used to build or train models, including the nature of the use, its objectives, its scope, the sources of data, and, to the extent possible, the categories of affected individuals.
- Practical mechanisms to enable rights such as objection, withdrawal of consent, and erasure, while clarifying the technical and legal limits of these rights in specific cases and how to address them.
- Determination of the cases in which a Data Protection Impact Assessment (DPIA) is required before training or deployment, along with criteria for assessing the level of risk.
- Specification of mandatory mitigating measures when relying on legitimate interest or any other legal basis, including risk reduction controls, necessity and proportionality tests, and technical and organizational measures.
- A methodology for assessing whether the training outputs (or the model itself) have been anonymized or rendered nonidentifiable in a manner that prevents the extraction of personal data or the reidentification of individuals, and the consequences in cases of non-compliance.
- Clarifying the implications of training a model with data that has been collected or processed unlawfully, including the required corrective measures, compliance pathways, and responsibilities.

The guidance should also move beyond a narrow focus on direct individual harm to incorporate considerations of societal harm—such as discrimination, exclusion, stigmatization, and the impacts of profiling or predictive outcomes on specific groups. This would ensure a more balanced approach between the rights and interests of individual data subjects on the one hand, and the collective rights and interests of communities affected by model outputs on the other. Such considerations are particularly critical in high-sensitivity sectors, including digital public services, credit, employment, education, healthcare, and security.

In developing this guidance, reliance may be placed on international trends affirming that data protection principles – such as data minimization, purpose limitation, transparency, and riskbased governance – form the foundation for responsible artificial intelligence. Among these trends is the European Data Protection Board’s (EDPB) opinion on AI models and their relationship to data protection principles.

3. Legislative Proposals to Amend the Personal Data Protection Law

At the legislative level, the status of the Data Protection Center should be reconsidered to ensure genuine independence, strengthen trust in its decisions, and limit conflicts of interest. This may be achieved by amending the provisions governing its affiliation and governance structure to separate the Center from direct subordination to the competent minister.

The amendments should also guarantee a fixed term for the Center's chairperson, with protection against arbitrary dismissal, and rebalance the composition of its Board of Directors to ensure that it is not dominated by regulated entities or stakeholders with vested interests. The Board should include independent legal and technical expertise, as well as more balanced representation capable of safeguarding the Center's institutional neutrality.

The concerns regarding the scope of application call for reconsideration of the expanded exemptions, particularly those related to national security and to the Central Bank and entities subject to its supervision. The relevant provisions should be amended to avoid broad, vague standards and to confine any exemption to a clearly defined, necessary, and specific scope. Procedural and oversight safeguards should also be introduced to prevent these exemptions from becoming a gateway to blanket exclusions or non-reviewable orders.

Regarding the Central Bank exemption, the blanket exemption should be removed. The financial sector should be brought under the general data protection framework, while establishing an institutional coordination mechanism between the Data Protection Center and the sectoral regulator to avoid regulatory conflict. Financial data is highly sensitive and requires general safeguards no less than other categories of personal data.

This approach can be supported by international references. The GDPR permits the imposition of restrictions or exceptions on certain obligations and rights only by way of a legislative measure, and on condition that they respect the essence of fundamental rights and freedoms, and that the restrictions are necessary and proportionate in a democratic society to achieve specified purposes (such as national security or essential economic/financial interests).

The GDPR further requires that legislative measures providing for exceptions include specific safeguards, covering: the purpose of processing or categories of processing; the categories of data concerned; the scope of the restriction; safeguards to prevent misuse or unlawful access/transfer; the identification of the controller or categories of controllers; retention periods and their safeguards; an assessment of the risks to individuals' rights; and the right to notify the data subject of the restriction unless this would undermine its purpose.

In addition to comparative regulatory references, this approach can be grounded in a broader international humanrights framework. Article (17) of the International Covenant on Civil and Political Rights (ICCPR) establishes the right to privacy and prohibits any arbitrary or unlawful interference. United Nations humanrights mechanisms have consistently interpreted these two qualifiers as referring to the principles of legality, necessity, and proportionality. This means that any restriction must be prescribed by law; the law must clearly and specifically define the circumstances, limits, and safeguards of the interference; the restriction must serve a legitimate aim; it must be the least intrusive means and proportionate to the objective; and it must not deprive the essence of the right to privacy of its meaning.

Regarding the sanctions chapter of the Law, it is recommended to review the proportionality between penalties for serious acts and those for procedural violations. Severe penalties should be retained for intentional violations that strike at the essence of privacy protection, such as data trafficking or deliberate data leakage.

In contrast, it is recommended that administrative and regulatory violations of a correctable nature be addressed through graduated instruments closer to administrative sanctions or escalating fines, rather than expanding the scope of criminalization for procedural errors. This would contribute to achieving clearer criminal justice and enhance enforcement effectiveness by directing deterrence to areas of genuine risk.

In parallel, it is recommended to strengthen the right of individuals to compensation and redress by a more explicit legislative text that establishes the right of the affected party to fair compensation for material or moral damage resulting from a violation of data protection rules, thereby strengthening the position of individuals before the courts, creating a real incentive for compliance, and helping to develop judicial precedent that establishes rights-based standards for data protection.

4. Regulatory and Technical Improvements Enhancing Implementation, Capacity Building, and Transparency

It is recommended to develop a unified electronic platform for interactions with the Data Protection Center, enabling the submission and tracking of applications for licenses, authorizations, and accreditation certificates; the registration of data protection officers and the management of their records; the receipt, response to, and documentation of individuals' complaints; and, where appropriate, the electronic submission of documented requests by individuals to exercise their rights, while ensuring the platform's security and ease of use. This platform would serve as a tool to reduce bureaucratic friction, standardize procedures, and document them. It should include simplified awareness content for the public that explains rights and complaint mechanisms, as well as guidance content for companies and other entities outlining compliance steps and requirements.

It is also recommended that the Center's awarenessraising and training role be activated in a regular and institutionalized manner through the adoption of a published annual awarenessraising and training plan that targets, on the one hand, data protection officers and processing personnel and, on the other hand, the general public. This should include the development of guidance materials and simplified, usable templates – such as clear consent forms, guidance on withdrawing consent, model privacy policies, and mechanisms for handling access and erasure requests. It is also advisable to link the accreditation and renewal of data protection officers and consultants to periodic accredited training hours to ensure the development of cumulative expertise beyond the initial examination.

To enhance trust and transparency, it is recommended to adopt a policy of publishing the Center's substantive decisions in a redacted form that does not disclose personal data, along with periodic publication of statistics on the nature of complaints and their outcomes, patterns of violations, and inspection activities. This would provide the public, researchers, and legislative institutions with objective monitoring tools and reduce the risk of selectivity in enforcement.

Related to this is the need to establish a clear framework for the annual report on the state of data protection, specifying its publication date, its minimum content, and the mechanism for its publication and accessibility, so that the report becomes a tool of public accountability and a genuine indicator of the system's performance.

Finally, it is recommended to strengthen the technical infrastructure for data security by leveraging available resources to develop monitoring and assessment tools to help the Center perform its tasks efficiently. This includes developing capabilities for security auditing of information systems in highrisk entities, encouraging the adoption of strong encryption for stored and transmitted data, and improving the quality of technical compliance through feasible technical guidelines and standards. This can be complemented by developing early detection mechanisms for breaches and leaks in coordination with relevant authorities, thus supporting the shift from reactive enforcement to proactive prevention that minimizes harm to data subjects.

Conclusion

The Executive Regulations of the Egyptian Personal Data Protection Law represent a procedural extension of the law itself, through which the practical meaning of the right to privacy in the digital sphere is determined. Hence, the value of the regulations is measured by their ability to translate general obligations into measurable, accountable operational rules, and by the extent to which they effectively protect and narrow the power gap between the data subject and the entities capable of collecting, processing, and circulating their data.

The initial reading of the Regulations – in the period before their actual entry into force – reveals that protection problems do not arise only from the absence of principles; rather, they are often generated by the very design of procedures. This includes the way consent is defined and the mechanisms for its verification, the ease of its withdrawal, the time and financial cost of exercising rights, the breadth or vagueness of exemptions, and the excessive reliance on prior authorization as the sole gateway for control.

It is precisely at this level that the enforceability of the right is determined, because rights that lack clear pathways, binding deadlines, and inspectable records become a legal promise that the rightsholder has no means to operationalize.

Similarly, a regulatory framework that burdens compliance with general licensing procedures without a riskbased approach opens the door to formal compliance that completes paperwork but does not guarantee protection. It imposes on smaller actors a cost disproportionate to the nature of their processing, while at the same time confusing the regulatory authority's ability to enforce consistently and fairly.

Furthermore, a governance structure in which the tools of regulation, supervision, and enforcement are concentrated within a single body makes the guarantees of independence and transparency inseparable from the very essence of protection. The rightsbased standard is not limited to the existence of a strong supervisory authority; it extends to the conditions under which that authority exercises its power – such as the clarity of rules, the transparency of criteria, the availability of necessary public information to assess performance, and the possibility of effectively questioning, challenging, and appealing decisions.

When the frameworks for periodic reporting, institutional transparency, and community engagement are absent, the system's ability to build stable public trust declines, the capacity to track trends in violations and measure compliance weakens, and practice becomes closer to bureaucratic management of a sensitive file rather than a protection system grounded in legal certainty.

The importance of these considerations multiplies with the expanding use of data in emerging technologies and artificial intelligence, where risks are no longer limited to leakage or breaches but also include largescale reuse, classification, automated decisionmaking, and the direct or indirect harms that may result. Therefore, developing more specific operational criteria in this field and linking them to a clear methodology for risk management and impact assessment is a necessary condition to avoid widening the gap between the speed of technological transformation and the sluggishness of regulatory safeguards.

Therefore, developing a robust system to protect the right to privacy requires treating regulations as a dynamic framework, subject to reform and improvement. It is essential to emphasize that enhanced protection is not achieved by increasing abstract restrictions, but rather by improving the quality of procedural rules, standardizing and simplifying them where necessary, and by making the exercise of rights accessible, cost-effective, and achievable in practice.