Baker McKenzie.

Client Alert

January 2026

Egypt: Important Data Protection Update

Regulations issued under the Personal Data Protection Law

In brief

More than five years after the publication of Personal Data Protection Law No. 151 of 2020 (PDPL), the government of Egypt has issued the Executive Regulations to the PDPL by virtue of Minister of Telecommunications Decree No. 816 of 2025 ("**Regulations**"). This significant development clarifies when the PDPL comes into full force and effect, establishes new compliance requirements for businesses handling personal data in Egypt, and empowers the Personal Data Protection Center ("**Center**") as the supervisory authority responsible for implementing, monitoring and enforcing the PDPL.

Contents

Key takeaways

- The publication of the Regulations triggers the final stage of the PDPL implementation process and confirms the compliance deadline: in-scope organizations have a grace period to ensure compliance by 1 November 2026.
- The Regulations provide more clarity on a range of obligations that were introduced in the PDPL, including the following:
  - Licensing and permit regimes for controllers, processors, data transfers, electronic marketing and use of CCTV/visual surveillance systems in public places
  - Appointment and registration of an Egypt-based representative by controllers and processors based outside Egypt
  - Appointment and registration of a data protection officer by all controllers and processors
  - Process for notifying breaches within the timelines specified in the PDPL
  - Further details on the approval and consent process requirements for transfers of personal data outside Egypt
  - Enhanced restrictions on the use of children's data, with explicit consent from guardians required for processing the personal data of children under 15 years old
- In contrast to many international data protection regimes, the national supervisory authority has substantially more control as a result of the extensive licensing regime and approval requirements. These include the requirements for the Center to approve data collection and consent mechanisms for children's data, the mechanisms for exercising data subject rights, the accreditation (and potential removal) of data protection officers and the approval of foreign company representatives.
- Controller and processor licensing will be subject to tiered fees based on the number of "personal data records," with reduced fees for associations, unions and clubs. Permits are available for specific and temporary purposes, with tiered fee structures based on the number of personal data records and the length of the permit.
- Further direction and guidance may become available as the supervisory authority begins operating and progresses its licensing and supervisory functions.
- Most organizations will need to update their compliance frameworks to comply with the new conditions, procedures, documentation standards and approval steps, as discussed further below.

Recommended actions

Organizations with a local presence in Egypt, and any foreign entities handling, controlling or processing personal data in Egypt or relating to individuals in Egypt, fall within the scope of the PDPL and should consider the following immediate next steps:

- **Assess whether activities require a license or permit** as a controller, processor, electronic marketer or visual surveillance systems operator under the Regulations

- Undertake a **comprehensive assessment of personal data processing activities** and map them to the required governance, approval and recordkeeping requirements of the PDPL and the Regulations
- Confirm that their **data protection officer (DPO) structure, qualifications and independence** meet the regulatory requirements
- Determine whether an **Egypt-based representative** must be appointed for non-Egyptian entities processing data relating to individuals in Egypt
- Review **cross-border data flows** — including cloud routing, intragroup transfers and vendor processing — to identify where licenses/permits are required and ensure compliance with the new conditions and procedures
- Update **breach-response procedures** to reflect the relevant notification timelines
- **Review and update contracts** with controllers, processors and cloud providers to ensure alignment with PDPL obligations
- Ensure **training, documentation and other governance** measures are in place and meet the new inspection and audit expectations

In depth

The PDPL was issued in July 2020 and entered into force three months after publication, with a grace period for compliance extending until one year after the date of the issuance of executive regulations supplementing the law. It was anticipated that these regulations would be issued within six months of the effective date of the PDPL, but the Regulations were publicly released on 25 December 2025. The formal date of publication is 1 November 2025 (being the date of the official gazette in which the Regulations were circulated). Accordingly, we anticipate that the compliance grace period contemplated in the PDPL will extend until 1 November 2026.

Scope

All entities with a local presence in Egypt, and any foreign entities handling, controlling or processing personal data in Egypt or relating to individuals in Egypt, must now evaluate how the PDPL — as supplemented by the Regulations — applies to their operations and what must be done within the remainder of the PDPL's statutory grace period.

Key compliance requirements

The PDPL established a range of compliance requirements that have been further clarified by the Regulations:

- **Licensing and permits**: The Regulations introduce a comprehensive tiered licensing fee system for controllers and processors, with fees increasing according to the number of "personal data records" processed. Entities processing up to 100,000 records are exempt, but fees escalate in steps, reaching substantial amounts for very large datasets (up to EGP 666,666 (approximately USD 14,000) annually for more than five million records). Licenses are granted annually, while permits may be sought for shorter periods to allow processing of personal data or sensitive personal data for "specific and temporary purposes." Licenses or permits may also authorize cross-border transfers of personal data by the controller or processor (subject to compliance with the separate controls and standards on these transfers), with separate fees associated with cross-border transfer approvals. The Center has committed to notifying applicants of the approval or rejection of license/permit applications within 90 working days of the submission of all required information and documents. Renewal requests should be submitted at least three months prior to the expiry of any license term or one month prior to the expiry of any permit.
- **Marketing and surveillance**: Direct electronic marketing activities and the use of visual surveillance systems require a separate license or permit with fees set as a percentage of the main controller/processor license fee for direct marketing (10% for own marketing, 25% for marketing on behalf of others) or fixed amounts for the use of visual surveillance systems. The operation of CCTV or similar visual surveillance systems within private residences is excluded from this licensing requirement if the coverage of the system does not exceed the property boundaries.
- **DPO appointment**: As per the PDPL, all controllers and processors must appoint a DPO, and the Regulations introduce strict requirements for DPOs to be registered and approved by the Center, including rights for the Center to suspend a registered DPO and request their replacement. Any person wishing to be appointed as a DPO must hold relevant academic or professional qualifications, have practical experience and pass a test approved by the Center. Based on the test results, each DPO is assigned a unique identification code that is linked to the nature and volume of data they are authorized to handle. This suggests that, depending on their qualifications, each DPO will be permitted to manage only certain types and volumes of data, ensuring that data handling aligns with their expertise. This is a much more granular and competency-based approach than seen in many other jurisdictions but aligns with the tiered licensing structure set out in the Regulations. DPOs must submit an annual privacy protection report to the Center, and, in cases of replacement, a special report within 15 days of

assuming duties, formalizing ongoing oversight and accountability. DPOs may be subject to fines of up to EGP 2 million (approximately USD 42,000) under the PDPL for failure to fulfill their obligations.

- **Foreign entity representatives**: The PDPL requires controllers and processors outside Egypt to appoint a representative in the country. The Regulations make clear that this appointment must be made through a company branch or authorized office in Egypt and approved by the Center for the duration of the controller's/processor's license or permit.
- **Children's data**: The Regulations introduce new requirements for handling children's personal data. The PDPL already provided that children's data is considered sensitive personal data and that a legal guardian's consent is required for the processing of children's data. The Regulations clarify that holders, controllers or processors of data relating to children under the age of 15 must obtain explicit written consent from the guardian prior to processing this data for any purpose; consent may be obtained from either the child or the guardian if the child is aged between 15 and 18. In addition, consent mechanisms must be approved by the Center. Where a child participates in a game, contest or any other activity, no more data may be collected than is necessary for participation, and this data may not be used for profiling, tracking or behavioral monitoring of children.
- **Cross-border transfer controls**: Stringent controls in the Regulations require controllers or processors to obtain a license/permit from the Center and the consent of data subjects for cross-border data transfers. If the personal data is to be shared with a third-party controller or processor outside Egypt, the activities of the parties should be aligned to achieve a legitimate interest for both parties or the data subject, and precautions must be taken to ensure an equivalent level of legal and technical protection for the personal data to that applied under the PDPL. The Regulations do not introduce standard contractual clauses or other mechanisms to effect these safeguards, but they do allow for the Center to produce a list of countries that are deemed to offer adequate protection.
- **Breach notification timelines**: The PDPL establishes a strict 72-hour deadline for controllers or processors to notify the Center of any data breach or violation, or immediate notification in cases where the issue implicates national security considerations. The Regulations clarify that this notification should be made through the Center's designated electronic portal or hotline. Affected individuals should also be notified within three working days from the date that the breach is reported to the Center, using the agreed communication method at the time data collection consent was obtained.
- **Artificial intelligence (AI) model training**: The Regulations refer briefly to AI training, with a requirement for processors to handle personal data in accordance with "locally, regionally and internationally recognized principles" when using personal data for AI training and emerging or innovative technologies. Processors must ensure that these technologies are used in a manner that does not cause harm to the data subject.
- **Processor obligations**: The Regulations establish a range of obligations on processors that are more extensive when compared to other international data protection regimes. In addition to obligations to obtain a license/permit, appoint a DPO or representative, and notify data breaches (see above), processors are required to adopt technical and organizational measures that guarantee the ability to restore personal data, access it promptly, and contain it if there is a physical or technical incident. Processors also have recordkeeping and other governance obligations.
- **Digital evidence**: The Regulations include an article confirming that digital evidence derived from personal data will have the same probative value as evidence obtained from written data and information, subject to compliance with certain technical standards or conditions. This includes a requirement that the collection, extraction and preservation of the evidence must be performed by judicial enforcement officers authorized to handle this type of evidence or by experts from investigative or judicial authorities. This could place a significant administrative burden on the use of personal data in legal proceedings.

Next steps

Further practical details around implementation are likely to unfold as the Center becomes fully operational. The composition of the Center's board of directors is yet to be determined, and organizations should follow developments closely as the Center begins accepting applications and issuing guidance.

*****

Heba Samy, Associate, has contributed to this legal update.

Contact us

Ghada El Ehwany
Managing Partner
ghada.elehwany
@bakermckenzie.com

Dino Wilkinson
Partner
dino.wilkinson
@bakermckenzie.com

Lucrezia Lorenzini
Senior Associate
lucrezia.lorenzini
@bakermckenzie.com