LATHAM&WATKINS

Egypt's Personal Data Protection Regime vs. the GDPR: A Comparison

Organizations doing business in Egypt should note the differences between GDPR and PDPL requirements, including potential programs that may need uplift to ensure compliance.

November 2026



Introduction

Egypt enacted its first comprehensive data protection law, the Personal Data Protection Law No. 151/2020 (PDPL), which is supplemented by Executive Regulations No. 816 of 2025 (Regulations), on November 1, 2025. Together, the PDPL and the Regulations establish a comprehensive framework governing the collection, processing, storage, and transfer of personal data in Egypt. The Regulations introduce a tiered licensing system for data processing, cross-border data transfers, direct electronic marketing, and video surveillance systems, and elaborate requirements for consent, data protection officer (DPO) appointment, and breach reporting to the Personal Data Protection Centre (PDPC). These obligations are supplemented by a number of guidelines issued by the PDPC (Guidelines) to provide more guidance.

Applicability

Unlike the EU and UK General Data Protection Regulations (GDPR), the PDPL does not establish a general targeting threshold for applicability. Rather, it sets out the territorial scope of application based on the nationality/residency of the relevant persons and the circumstances of the breach. Accordingly, the PDPL has a much broader extraterritorial application than under the GDPR and applies to processing relating to:

- an Egyptian national, whether inside or outside Egypt (i.e., extraterritoriality based on nationality);
- persons (including non-Egyptian nationals) residing in Egypt; and
- a non-Egyptian outside Egypt, where the relevant act constitutes an offense in the jurisdiction where it occurred and the affected data subject is an Egyptian national or a non-Egyptian residing in Egypt.

Therefore, the PDPL applies to foreign entities processing personal data outside Egypt where the above conditions are satisfied (i.e., a nexus to Egyptian nationals or persons residing in Egypt exists), even if such entities do not have a physical presence in Egypt.

Grace Period

The Regulations established a grace period from November 1, 2025, to October 31, 2026, during which legal and enforcement risk remained relatively low. While the enforcement risk may be manageable in the short term, we expect the legal and enforcement risk to increase significantly after the grace period. From November 1, 2026, failure to comply with requirements under the PDPL may subject organizations to criminal and/or financial penalties (further explained below).

Organizations should work to align their current data privacy programs with key requirements under the PDPL and Regulations (such as obtaining required licenses/permits, implementing PDPC-approved consent mechanisms, appointing and registering a DPO, and establishing breach notification protocols) in order to minimize future compliance risks.

Practical Impact on Existing Privacy Compliance Programs

The PDPL and Regulations signal a major change in the way personal data is processed in or relates to Egypt. Organizations operating in Egypt or processing data of Egyptian nationals or residents in Egypt will want to review current privacy compliance programs against the new framework and consider steps to bring their privacy compliance in line with the PDPL. A GDPR-compliant entity has a strong base, as core data protection principles are broadly aligned, but Egypt introduces procedural and licensing requirements that require greater regulatory oversight as part of organizations' daily business operations that are not found under the GDPR. See below key elements of the PDPL and Regulations.

Material Scope

The PDPL covers personal data in a manner broadly consistent with the GDPR's approach. However, the PDPL covers only personal data that is processed electronically through fully or partially automated means. Further, the PDPL's definition of sensitive personal data is broader than under the GDPR (differences underlined). Sensitive personal data under the PDPL means "data which discloses psychological, mental, or physical health, or genetic, biometric or **financial data**, religious beliefs, political views, or criminal records. In all cases, **data relating to children is considered to be sensitive personal data**" (emphasis added).

Legal Bases for the Processing of Personal Data

The PDPL recognizes consent, fulfillment of contractual obligation, fulfillment of legal obligation, legitimate interest, claim or defense of a legal right, and execution of court judgments or orders from competent investigative authorities as lawful bases for processing. Egypt's approach closely mirrors the GDPR by recognizing contractual necessity and legitimate interests. However, where controllers rely on consent, PDPC approval of consent mechanisms is required as a prerequisite for obtaining any personal data processing license/permit.

Licensing Regime

The most significant divergence from the GDPR is the licensing regime introduced by the PDPL, which is now partially operational under the Regulations. The electronic portal established for this purpose has launched but is still in its testing phase. The licensing process for foreign entities is conducted offline and completed in person until the electronic portal is fully operational to provide its services to foreigners. The Regulations and the PDPC's guidelines on licenses and permits establish a tiered licensing system comprising (i) a general license or permit for personal data (including sensitive personal data) processing — which is a prerequisite for engaging in any processing activity (Main License/Permit); and (ii) supplementary licenses or permits, which are granted to engage in specific processing activities that require additional approvals, i.e., for cross-border data transfers, direct electronic marketing, and video surveillance.

Licenses or permits are on a per-entity basis (not per product). Annual fees are determined primarily by volume of personal data records. The PDPL licensing regime has no equivalent under the GDPR, representing a material divergence and potential compliance gap for multinational organizations. If the processing is on a temporary/limited basis, organizations need to apply for a *permit* instead of a *license.*

Local Representative

Foreign controllers or processors without a branch or representative office in Egypt must appoint a local representative accredited by the PDPC for the license/permit period. The appointed representative shall be officially registered by the PDPC for the duration of the license or permit.

DPO Appointment and Registration

DPO appointment is mandatory under the Regulations for all controllers and processors, regardless of processing volume or type. DPOs must also register with the PDPC via its DPO registry. The PDPC specifies mandatory qualification, experience, and integrity (i.e., clean criminal record) requirements for DPO registration, including passing the official examinations administered or accredited by the PDPC (even where the individual holds other qualifications, such as CIPP/E or CIPM).

The PDPC has recently started the DPO registration process, including conducting the examinations in person, and is preparing its DPO registry; registration is conducted in person until the electronic portal is fully operational. Controllers/processors must notify the PDPC of DPO termination/replacement and ensure uninterrupted coverage. This is materially different and broader than the GDPR, which requires DPOs only in defined scenarios and does not impose mandatory examinations for DPOs. Accordingly, multinational organizations may find it difficult to leverage their existing global DPOs to act as the local DPO for the PDPL's purpose.

Data Subject Rights

Data subjects under the PDPL have rights that broadly align with GDPR rights, including rights of access, rectification, erasure, and the right to lodge a complaint with the PDPC. The PDPL imposes obligations on controllers to facilitate the exercise of these rights and acknowledge the data subject's request within six business days. Specific rights available under the GDPR, such as the right not to be subject to automated decision-making, are not expressly provided for under the PDPL.

Cross-Border Data Transfers

Transfer, storage, sharing, processing, or granting access to personal data outside Egypt requires compliance with PDPL and Regulations controls, including obtaining a PDPC license/permit for cross-border data transfers, data subject consent (if consent constitutes the legal basis for processing), and implementation of appropriate safeguards (e.g., standard contractual clauses (SCCs) / binding corporate rules (BCRs), and a

transfer impact assessment (TIA)) to ensure a level of protection no less protective than that of the PDPL. Transfers may only be made to jurisdictions specified in the license/permit.

The PDPC is expected to issue a whitelist of countries with adequate personal data protection equivalent to that under the PDPL (similar to the European Commission's adequacy decisions), and transfers to whitelist countries will not require additional safeguards. Further, the PDPL does not confirm whether EU SCCs and BCRs will be deemed as sufficient under the PDPL — we expect more clarity on this once the PDPC begins reviewing license applications after the grace period and the licensing portal becomes fully operational. This represents a material gap from the GDPR's adequacy/SCC/TIA transfer model.

Data Breach Notification

Unlike the GDPR, the PDPL imposes no materiality threshold for notifying personal data breaches. This means that technically *all personal data breaches*, no matter how insignificant, need to be notified to the PDPC. Organizations must notify the PDPC within 72 hours of becoming aware of a personal data breach and data subjects within three business days after notifying the PDPC. If the breach relates to national security, enhanced notification obligations apply whereby the notification must be made immediately. The Egyptian Anti-Cybercrime Law No. 175 of 2018 separately requires immediate notification to the Egyptian Computer Emergency Readiness Team (CERT) for data/cybersecurity breaches.

Direct Electronic Marketing

Both creators and senders of direct electronic marketing (as the case may be and whether acting as controller or processor) must obtain a PDPC license/permit. Explicit data subject consent is required and cannot be bundled with general consent. Marketing communications must identify the sender and marketing purpose at the outset and allow refusal/withdrawal through PDPC-approved methods, including direct messages via social media platforms, short text messages, electronic mail, telephone calls, or any other approved technological means.

Consequences of Non-Compliance

Non-compliance may trigger administrative, civil, and criminal liabilities cumulatively. Penalties range from EGP 100,000 (approximately US$2,000) to EGP 5 million (approximately US$100,000) in fines, and certain violations may attract imprisonment of at least three to six months. The PDPC may also impose disciplinary measures, including partial or complete license suspension, and in more serious or persistent cases, permanent revocation. This includes cases where licensing requirements are not met, renewal fees are not paid, or the license is unlawfully transmitted to a third party. (Director- and manager-level personnel within the organization may also incur personal criminal liability if they were aware of the violation and their failure to discharge their management duties contributed to the commission of the offense.)

The PDPC and Egyptian courts have certain enforcement routes against offshore entities, including blocking access to websites/apps/platforms in Egypt, and enforcement against any assets owned by the offshore entity in Egypt. Taking reference from similar regulatory regimes in Egypt (e.g., media regulation) and based on current practice, the practical risk of enforcement against offshore entities with no physical presence in Egypt appears moderate to low, but is of course subject to change. However, this may change after the grace period, depending on how the PDPC enforces the PDPL against offshore entities.

The table below compares the requirements of the GDPR and the PDPL/Regulations in further detail, highlighting potential gaps in GDPR-based compliance programs and outlining possible steps to uplift such programs for PDPL compliance purposes. As additional regulatory guidance is issued by the PDPC, organizations may need to adjust their compliance approaches accordingly.

The table is color-coded as below for ease of reference:

Minimal difference: The PDPL is materially consistent with the GDPR. No further action is required to comply with the PDPL.

No-action gaps: The PDPL is generally consistent with the GDPR, but with noticeable differences. The GDPR standard is higher or more comprehensive. Additional compliance actions will not be required to comply with the PDPL.

Manageable gaps: The PDPL is generally consistent with the GDPR, but with noticeable differences. Minor additional compliance actions are required to comply with the PDPL.

Material gaps: The PDPL is materially different from the GDPR. There are elements under one law that are not found under the other. Significant additional compliance actions are required to comply with the PDPL.

The PDPL vs. the GDPR

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
Scope of application							
1.	**Territorial applicability**	✓	The GDPR applies to the processing of personal data (i) in the context of the activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU; and (ii) by a controller or processor not established in the EU, where the processing relates to offering goods or services to data subjects in the EU, or monitoring their behavior as far as it takes place within the EU (i.e., the targeting criterion). Applicability is not based on the nationality of the data subject.	✓	The PDPL does not establish a general targeting threshold. Instead, it applies based on the nationality/residency of the relevant persons and applies to processing relating to (i) an Egyptian national, whether inside or outside Egypt; (ii) persons (including non-Egyptian nationals) residing in Egypt; and (iii) a non-Egyptian outside Egypt, where the relevant act constitutes an offense in the jurisdiction where it occurred and the affected data subject is an Egyptian national or a non-Egyptian residing in Egypt. The PDPL therefore applies to foreign entities processing personal data outside Egypt where there is a nexus to	**Material gaps:** The PDPL has a much broader extraterritorial reach than the GDPR. Under the GDPR, an offshore organization is generally only caught if it targets or monitors individuals in the EU, whereas the PDPL may apply to any processing of personal data of Egyptian nationals (wherever located) or persons residing in Egypt, without any targeting or establishment requirement. Organizations that fall outside the GDPR's territorial scope may therefore still be subject to the PDPL.	• Map whether personal data of Egyptian nationals (inside or outside Egypt) or persons residing in Egypt is processed, including by group entities and service providers with no presence in Egypt. • Do not rely on the absence of an Egyptian establishment or targeting activity as a basis for concluding that the PDPL does not apply; where an Egyptian nexus exists, assess compliance with the PDPL (including the licensing requirements).

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					Egyptian nationals or persons residing in Egypt, even if such entities have no physical presence in Egypt.		
2.	**Personal data**	✓	Any information relating to an identified or identifiable natural person.	✓	Personal data in electronic form relating to an identified or identifiable natural person.	**Minimal difference**	N/A
3.	**Sensitive / special-category personal data**	✓	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.	✓	Data that discloses psychological, mental, or physical health; genetic, biometric, or financial data; religious beliefs, political views, or criminal records. In all cases, data relating to children is considered to be sensitive personal data. To process sensitive personal data, controllers/ processors must obtain a license/permit for sensitive data processing (this forms part of the general data processing licensing), obtain explicit written consent where consent is the legal basis, ensure data is essential and necessary, comply with PDPC security standards, and maintain secure electronic registers.	**Material gaps:** Egypt's definition of sensitive personal data is broader than that under the GDPR, as it includes financial data (e.g., bank account information, credit card information) and all personal data of children under 18 years old. The PDPL also imposes a licensing requirement for sensitive data processing (this forms part of the licensing requirement for general data processing), which is not found under the GDPR.	• Review whether financial data or children's data is processed and ensure that safeguards for processing sensitive personal data are implemented. • Check whether Egyptian national IDs are collected (these are mandatory for all Egyptian nationals) as they contain religious data, which is a form of sensitive personal data. • Ensure license/permit scope covers sensitive data processing activities. • Obtain explicit written consent where consent is the legal basis for sensitive data processing. • Implement and maintain appropriate technical and organizational measures to safeguard sensitive data in storage.
4.	**Data subjects**	✓	The identified or identifiable natural person to whom personal data relates.	✓	The identified or identifiable natural person to whom personal data relates.	**Minimal difference**	N/A

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
5.	**Data holder**	✗	There is no equivalent concept under the GDPR.	✓	Any natural or legal person who legally or factually possesses and retains personal data in any form or on any storage medium, whether such person is the originator of the data or has acquired possession thereof by any means.	**Material gaps:** Under the GDPR, there is no concept of a "data holder," a party who merely possesses or retains data without determining purposes/means or processing on behalf of a controller.	• Assess whether any entity qualifies as a data holder under the PDPL. • The PDPL requires data holders to: (i) if requested to disclose personal data, ensure the request is submitted in writing by an authorized party or pursuant to a legal provision, verify the validity of, and retain, the documents necessary to effect the disclosure, and respond to the request within six working days of submission; (ii) if holding personal data relating to children, obtain the explicit consent of the data subject's legal guardian; and (iii) respond to and acknowledge data subject requests within six working days.
6.	**Data controller**	✓	The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data.	✓	Any natural or legal person that, by virtue or nature of their work, has the right to access personal data and determine the purposes and means of retaining and processing personal data.	**Minimal difference**	N/A
7.	**Data processor**	✓	A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.	✓	A person that processes personal data for their own benefit or on behalf of the controller.	**Minimal difference**	The PDPL definition captures a person processing personal data "for their own benefit," which under the GDPR would generally indicate controller status; this may create characterization issues (e.g., a vendor engaged as a

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
							processor that also uses the data for its own purposes), so roles should be assessed under each regime separately.
8.	**Processing**	✓	Any operation or set of operations that is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.	✓	Any electronic or technical operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment, combination, indexing, sharing, disclosure by transmission, dissemination, or otherwise making available, restriction, erasure, or destruction, through any electronic or technological medium or device.	**Manageable gaps:** Purely manual, non-electronic processing (e.g., paper-only filing systems with no digital component) falls outside the PDPL's scope. The GDPR applies to processing "by automated means" and to non-automated processing of personal data forming part of a filing system, which covers manual filing systems.	N/A
9.	**Processing children's data**	✓	The GDPR contains provisions to enhance the protection of children's personal data: • If transparency information is intended to be read by a child, it should be in clear and plain language that children can easily comprehend. • If an information society service is offered to a child,	✓	The age of majority in Egypt is 18. This means that those under 18 years old are considered children. Personal data relating to children is classified as sensitive personal data and subject to certain protective safeguards. For a child under 15 years old, consent must be provided only by the parent/legal guardian. For a child aged 15-18, consent may be provided by either	**Material gaps:** Egypt classifies all children's data (those up to 18) as sensitive personal data, thereby subjecting the processing of such data to more protective safeguards. While the age of majority is generally 18 in both Egypt and the EU, the PDPL treats all individuals up to 18 as children for data protection purposes. By contrast, the GDPR	• Obtain parental consent for the processing of children's (under-15's) personal data, where relying on consent as the legal basis. • Obtain parental consent or the explicit consent of the child for the processing of children's (those from 15 to 18) personal data, where relying on consent as the legal basis. • Review existing age verification measures and

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			consent should be obtained from a parent/guardian, subject to certain age criteria. The age of majority is not defined under the GDPR, and it varies across EU Member States. However, certain provisions are applicable to children under the age of 16.		the child or the parent/legal guardian, provided the parent/legal guardian is aware of the child's consent. When processing personal data of children (all of which qualify as sensitive personal data) or if there is suspected processing of personal data of children, the controller is required to employ age verification measures to establish proportionate verification processes to determine whether the data subject meets the required age threshold or whether guardian consent is necessary. **Age Gate and Parental Consent Method** The prevailing market practice for age verification in Egypt is self-declaration, mobile carrier verification, and parental consent.	does not define a child, and the Art. 8 age of digital consent for information society services ranges between 13–16 depending on the EU Member State. Under the PDPL, the equivalent consent threshold is effectively 15, with parental/guardian awareness required for children aged 15 to 18.	apply 18 as the minimum age threshold in Egypt. • Ensure the license or permit obtained from the PDPC regarding processing of personal data covers the processing for sensitive personal data (i.e., children's data).
Licensing regime (Egypt-specific)							
10.	**General processing license/permit (Main License/ Permit)**	✗	There is no equivalent concept under the GDPR. The GDPR does not require controllers or processors to obtain prior authorization or licensing from a data protection authority before processing personal data (with limited exceptions for	✓	Controllers and processors must obtain a Main License or Permit (i.e., controller license/permit, processor license/permit, or consolidated controller and processor license/permit) from the PDPC before processing personal data, including sensitive personal	**Material gaps:** The PDPL's mandatory licensing regime has no equivalent under the GDPR. This represents one of the most significant divergences from the	• Organizations should prepare for the licensing application by conducting a fact-finding exercise and engaging local Egyptian counsel for assistance, as well as preparing the required documents and data to be submitted at the time of the application.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			prior consultation following a DPIA).		data. This is a prerequisite for processing any personal data. **License Application** • Licenses are on a per-entity basis (not per product). • The PDPC applies a two-stage licensing process: the Main License/Permit must be obtained first before applying for any supplementary license/permit (cross-border transfer, direct electronic marketing, or video surveillance). It is unclear whether the portal will allow simultaneous submission of applications. • Licenses are granted for a period of three years. An application for renewal must be submitted at least three months prior to the license expiration date. • Applications are submitted in accordance with the controller's and processor's legal status and must specify the purpose of processing, the	GDPR and compliance gaps for multinational organizations.	• The electronic portal has launched and is partially operational; however, it is still in its testing phase. As at October 2026, the licensing process for foreign entities is conducted offline and completed in person, until the electronic portal is fully operational.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					categories and volume of personal data involved, and the technical and organizational measures implemented to ensure compliance with the PDPL. • The PDPC retains discretion to request additional information or safeguards and to impose conditions on the scope or duration of the authorization granted. • If changes occur to any element of the processing operations, the license or permit holder shall submit a request to the PDPC to amend their license or permit. **Permits** • Temporary permits are available for short-term/limited activities not exceeding one calendar year, such as pilot programs and specific projects not covered by main license and timebound processing activities.		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• Permits are granted for a period of either three, six, nine, or 12 months. An application for renewal must be submitted at least one month prior to the permit expiration date. • Permit fees would also be determined according to the requested duration and volume of personal data involved. Records totaling up to 25,000 would be exempt from fees. • If changes occur to any element of the processing operations, the license or permit holder shall submit a request to the PDPC to amend their license or permit. **License Fees** • Annual fees are determined primarily by volume of personal data records: no fees apply for up to 100,000 records; beyond this, fees increase progressively and range approximately from EGP 200 (approx. US$4) (for up to 200,000 records) to		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					EGP 1,000 (approx. US$20) (for up to 1 million records). • For data volumes exceeding 5 million records, the maximum license fee would be the legally prescribed cap of EGP 666,666 (approx. US$13,333) annually, totaling EGP 2 million (approx. US$40,000) over three years. • Controller-only or processor-only licenses reduce applicable fees by 50%. **Enforcement Risk** • In the short term, if an organization complies with the key requirements of the PDPL except for the license requirements, the enforcement risk is likely manageable; especially if the organization can demonstrate that it is preparing for the license application. • In the long term, the enforcement risk is likely high on the basis of the high legal risk and consequences of non-compliance (fines		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					ranging from EGP 500,000 (approx. US$10,000) to EGP 5 million (approx. US$100,000), and the person responsible for the actual management of the legal entity may also incur personal criminal liability if they were aware of the violation and their failure to discharge their management duties contributed to the commission of the offense). There are currently no published enforcement actions or judicial precedents relating to these requirements, particularly against offshore controllers, as the regulatory framework is relatively new.		
11.	**Supplementary license/permit: cross-border data transfers**	✗	No equivalent. The GDPR relies on adequacy decisions, SCCs, BCRs, and other transfer mechanisms rather than a licensing/permit system.	✓	Any transfer outside Egypt, including cloud/server processing, remote access, or storage abroad, requires prior PDPC authorization via the supplementary license/ permit. This requirement is absolute and applies irrespective of whether the transfer is to a whitelist country or whether appropriate safeguards (e.g., SCCs and transfer impact	**Material gaps:** There is no GDPR equivalent to Egypt's mandatory licensing for cross-border transfers. This is a fundamental departure from the GDPR's SCC/BCR approach. The compliance burden associated with such licensing creates a de facto data localization requirement.	• Map all jurisdictions to which Egyptian personal data is transferred, stored, or processed. • Prepare and submit cross-border supplementary license/permit application(s) identifying all destination jurisdictions. • Gather supporting documentation (compliance evidence, foreign recipient contracts, consent proof).

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					assessment (TIA)) are in place. Transfers may only be made to jurisdictions specified in the license/permit. For new recipient jurisdictions that are not mentioned in the license/ permit, the organization would need to notify the PDPC and obtain its approval by updating the license and the original application. In determining what jurisdictions to approve for the PDPC license and cross-border transfer of data, the PDPC considers existing legislation or controls, their extent of practical consistency, availability of security measures, and availability of laws specific to compensation for damages suffered for misuse of personal data. This analysis would typically form part of the TIA, which would also need to be submitted to the PDPC as part of the application if the recipient jurisdiction is not a whitelist country. **License Application** • License applicants will have to specify the destination of transfer, nature and purpose of		• Establish a process to update the license when new jurisdictions are needed.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					the transfer, describe security systems and storage locations, and submit proof of compliance. • Organizations also need to submit proof of the nature of the controller's/processor's activity to which the data is transferred. They would also provide a description of categories of personal data transferred, their volume, and retention period. The application fee is 50% of the relevant Main License/ Permit fee.		
12.	**Supplementary license/permit: direct electronic marketing**	✗	No equivalent licensing concept. Under the GDPR, direct marketing requires a lawful basis (typically consent or legitimate interests), and data subjects have an absolute right to object to processing for direct marketing at any time, which must be explicitly brought to their attention. Separately, the ePrivacy Directive (ePD) (as implemented in EU Member States) and the UK's Privacy and	✓	Creators/senders of direct electronic marketing must obtain a PDPC license/permit. **License Requirements** Such license or permit authorizes the use of personal data for direct electronic marketing activities, whether for the licensee's own purposes or on behalf of third parties. There are two categories of direct electronic marketing (DEM) licenses/permits: 1. **License/permit for DEM for Others:** if the	**Material gaps:** The GDPR/ePD framework does not require a license for direct marketing activities.	• Determine whether direct electronic marketing activities involve processing of Egyptian personal data or of non-Egyptians resident in Egypt. • If an organization (creator) uses a marketing intermediary (service provider) to send direct marketing, inquire as to whether the intermediary has obtained the relevant DEM license. This would be a practical way of satisfying the requirement without the organization having to obtain the license itself.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			Electronic Communications Regulations 2003 (PECR) generally require prior opt-in consent (to the GDPR standard) for unsolicited electronic marketing (e.g., email, SMS) to individuals, subject to a "soft opt-in" exception for marketing similar products/services to existing customers whose contact details were obtained in the context of a sale, provided they were given a simple means to opt out at collection and in each subsequent message. Each communication must identify the sender and provide a valid address for opt-out requests. Rules for B2B marketing and telephone marketing vary between Member States.		controller/processor promotes goods/ services/activities of third parties (e.g., a customer). Fee would be 25% of the Main License fee. 2. **License/permit for DEM for Oneself:** if the controller/processor promotes their own goods/services. Fee would be 10% of Main License/Permit fee. **DEM Requirements** • The license/permit requirement is separate to the requirement to obtain explicit consent from data subjects before using their personal data for direct marketing and prior to sending any electronic direct marketing communications. • Personal data must be permanently erased when consent is withdrawn, the retention expires, or the direct marketing purpose ends. • Marketing communications must identify the sender and marketing purposes at the outset.		• Senders (e.g., marketing intermediaries) whose primary business activity involves sending direct marketing to Egyptian data subjects or to non-Egyptians resident in Egypt should apply for a direct marketing PDPC supplementary license. • Organizations should review their existing direct marketing framework and ensure compliance with requirements (particularly on explicit consent).

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• Allow refusal/withdrawal through PDPC-approved methods (social media DMs, SMS, email, calls, or other approved technologies). • Marketing intermediaries must verify consent and retain evidence or cease use. • The creator shall maintain updated and accurate electronic records of all opt-out (withdrawal) requests received. • The sender shall maintain electronic records, which shall be made available to the PDPC upon request. The electronic records shall include (i) the method and date of the data subject's consent to receive marketing communications, including the specific marketing purpose; (ii) any requests submitted by the data subject for erasure, modification, or withdrawal of consent and the actions taken in response thereto; and (iii) the technical and		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					organizational measures implemented to ensure the security and protection of personal data in accordance with the procedures approved by the PDPC. These records must be retained for a period of three years from the date of the last electronic direct marketing communication sent to the data subject.		
13.	**Supplementary license/permit: CCTV/video surveillance systems**	✗	No equivalent licensing concept.	✓	A supplementary license/permit for video surveillance systems is required for those who use or intend to use video surveillance systems, including CCTV, through which images or videos of individuals may be captured in public areas and which can identify them.	**Material gaps:** The GDPR/ePD framework does not require a license for using CCTV.	• Organizations to review whether they use CCTV that would capture Egyptian data subjects. If so, apply for a supplementary license/ permit. This license is most relevant for employers (e.g., CCTV at workplace if considered a public space) and for organizations that use CCTV in public spaces (e.g., shopping malls).
Transparency							
14.	**Privacy policy disclosures**	✓	Data subjects must be informed of the following at the time of collection of personal data: • name and contact details of the data controller and local	✓	Privacy notices must include: • the identity and contact details of the controller and/or processor; • the contact details of the DPO;	**Manageable gaps**	• Update privacy notices to include cross-border transfer legal basis and PDPC complaint rights.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			representative (if applicable); • contact details of the DPO; • purposes of processing; • lawful basis for processing and legitimate interests for processing (if applicable); • categories of personal data obtained; • recipients of personal data; • details of transfers of personal data to any third countries or international organizations; • retention periods for personal data; • data subject rights; • right to withdraw consent (if applicable); • right to lodge a complaint with a supervisory authority; • source of personal data (if personal data is not obtained from the individual it relates to); • details of whether individuals are under		• the lawful basis of processing; • the categories of personal data collected; • the purpose(s) of processing; • the recipients or categories of recipients of the personal data, if applicable; • the legal basis (e.g., consent, contractual/legal obligation, legitimate interest, etc.) for cross-border transfers, and the jurisdictions to which the data is transferred, if applicable; • the retention period of processing, or criteria of determining such retention period, or a cross-reference to the retention policy; • data subjects' rights and how to exercise them; • where the data is collected indirectly, the source from which the personal data was collected, or, if not possible, a general description of the categories of sources, where multiple sources		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to); and • details of the existence of automated decision-making, including profiling (if applicable).		are used (e.g., social media platforms); and • the right to lodge complaints with the PDPC. Notices must be in clear and plain language, distinct from other information.		
15.	**Language requirements**	✓	Information provided to data subjects must be in clear and plain language (including the native language of the data subject, when required).	✓	The PDPL does not contain an express language requirement; however, pursuant to the Guidelines, information provided to the data subject regarding the processing activity provided in, *inter alia*, privacy notices must be in Arabic as the primary language, in addition to being clearly defined (neither vague nor bundled). Other languages may be added depending on the intended audience. Furthermore, the request for consent must be provided in Arabic in order to be valid. Data controllers and processors are free to add other languages depending on their business needs.	**Manageable gaps**	• Ensure privacy notices and requests for consent are available in Arabic.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
Legal basis of processing							
16.	**Consent**	✓	**Consent** Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signify agreement to the processing of personal data relating to them. **Explicit Consent** Undefined, but must be affirmed in a clear statement and needs to refer to the element of the processing that requires explicit consent.	✓	A valid consent must be: • provided directly by the data subject or authorized legal representative; • explicit; • adequately informed; • separately and specific to each processing purpose; • freely given without the data subject feeling coerced or compelled; and • documented with consent logs available to the PDPC on request. A valid consent for the processing of sensitive personal data must be: • written; and • obtained from the legal guardian (if the personal data relates to children). **Unbundled Consent** Consent requests must be standalone and separate from general terms and conditions/privacy policy (i.e., unbundled). In particular, the purpose of processing must be clearly defined and not vague or bundled. Separate	**Manageable gaps:** The core consent standard is broadly aligned (free, specific, informed, unambiguous). However, Egypt imposes a unique requirement for PDPC approval of consent mechanisms before any Main License is granted.	• Obtain PDPC approval for consent obtaining mechanisms. • Ensure consent requests are standalone, unbundled, and clearly defined. • Implement mandatory consent record-keeping with required fields (identity, timestamp, information provided, affirmative action, withdrawal details). • Review existing consents for compliance; refresh if not meeting PDPL standards. • Keep electronic records of the consent and ensure consent flows, including the notice provided to users, the manner in which consent is obtained, and the record kept of it, are documented in a form capable of being submitted in support of a license/permit application once the PDPC opens the licensing process.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					consents must be obtained for each distinct processing activity, with each request clearly explaining the type of processing and its corresponding purpose. While neither the PDPL and Regulations, nor the PDPC guidelines require a separate tick box for each processing purpose, separate tick boxes would be the most straightforward way to demonstrate compliance with these requirements. Other mechanisms may also be acceptable, provided they clearly enable the data subject to give separate and specific consent for each purpose and, where applicable, for the cross-border transfer of personal data. **PDPC Approval** Where controllers rely on consent as a legal basis, they must seek PDPC approval of the consent mechanism as part of the Main License/Permit application review — the PDPC will review an organization's consent framework (i.e., how it obtains consent) as part of its Main License/Permit application. This does not operate as a standalone		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					approval / separate filing. In the Main License/Permit application process, the applicant will be required to provide details of the mechanism used to obtain consent as a condition for the license/permit. **Electronic Consent Records** Electronic consent records must be accurate, regularly updated, and made available to the PDPC upon request, and must include, at minimum: • data subject name or unique identifier; • date and time (digital timestamp); • information provided in consent request; • affirmative action taken by the data subject to authorize the processing; and • whether the data subject has exercised the right to withdraw consent (if so, date and time of withdrawal). Prior consent obtained may not need a refresh if it meets requirements and is recorded, provided that the consent remains valid and up-to-date, and reflects the processing activity.		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
17.	**Contract**	✓	Processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.	✓	Fulfillment of contractual obligation is recognized as a legal basis for processing under the PDPL. This lawful basis applies where the processing of personal data is required for the performance of a contract to which the data subject is a party, or to take steps to enter into such a contract.	**Minimal difference**	N/A
18.	**Legal obligation**	✓	Processing is necessary for compliance with a legal obligation to which the controller is subject.	✓	Fulfillment of legal obligation is recognized as a legal basis for processing under the PDPL.	**Minimal difference**	N/A
19.	**Vital interests**	✓	Processing is necessary to protect the vital interests of the data subject or of another natural person.	✗	The PDPL does not expressly recognize this as a standalone legal basis for processing.	**Material gaps**	• Obtain explicit consent of data subject if this basis will be used for the cross-border transfer of data.
20.	**Public interest**	✓	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	✗	The PDPL does not expressly recognize this as a standalone legal basis for processing.	**No-action gap:** The PDPL does not provide a standalone "public interest" legal basis equivalent to Art. 6(1)(e) GDPR. However, public interest processing is likely subsumed under the broader legal obligation / court order basis.	• Obtain the explicit consent of the data subject if this basis will be used for the cross-border transfer of data.
21.	**Legitimate interests**	✓	Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where overridden by the interests or fundamental	✓	Legitimate interest is recognized as a legal basis under the PDPL. To rely on legitimate interests, a legitimate interests assessment should	**Manageable gaps**	• Document legitimate interest assessments in a manner consistent with PDPL requirements. • Monitor PDPC guidance on the scope and application of

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			rights and freedoms of the data subject that requires protection of personal data, in particular if the data subject is a child. To rely on legitimate interests, a legitimate interests assessment should be carried out.		be carried out, balancing out the organization's legitimate interest against the rights and interests of the data subject, to ensure the following cumulative conditions are met per the Guidelines: • The interest pursued by the controller or processor must be legitimate (legitimacy). • The processing activity must be strictly necessary to achieve the pursued interest (necessity). • The processing activity must be proportionate to ensure that the pursued interest does not override the data subject's rights and freedoms (proportionality).		legitimate interests under Egyptian law.
22.	**Claim or defense of a legal right**	✓	There is no equivalent legal basis for the processing of personal data under Article 6. However, this is available as a basis for processing special-category data under Article 9(2)(f), where necessary for the establishment, exercise, or defense of legal claims.	✓	Under Article 6(2) PDPL, the claim or defense of a legal right is recognized as a standalone legal basis for processing.	**Minimal difference**	N/A

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
Data processing agreements / controller-processor obligations							
23.	**Controller-processor contracts**	✓	Under Article 28, processors must process personal data in accordance with a contract that requires that the processor: • processes personal data in accordance with agreed purpose(s) and on instruction of the controller; • returns or destroys personal data upon termination; • obtains approval prior to contracting with sub-processors; • implements necessary measures to ensure the security of personal data; • submits to audits and inspections; • provides assistance to the controller to fulfill obligations under the GDPR; and • notifies the data controller as soon as reasonably possible upon discovering a security breach.	✓	There is no equivalent to Article 28 GDPR under the PDPL that prescribes the mandatory contractual obligations that a controller must include in its data processing agreement (DPA) with the processor. However, the Guidelines have provided that in order to ensure consistency with the data protection regulatory frameworks and applicable laws and regulations, agreements between data controllers and processors may include the following: • scope and limitations, *inter alia*, the purpose(s) of the processing activity and the categories of personal data; • data protection undertakings specifying each party's obligations; • audit and inspection rights; • assistance with data subject requests; • security measures to be implemented; • procedures for data breach notifications;	**No-action gaps:** The obligations on processors are broadly consistent with GDPR Article 28 requirements, although there is no express obligation on controllers to flow down processor obligations in their DPAs with processors, albeit this is likely implied given the direct obligations on processors. As such, putting aside the license requirement, existing GDPR-compliant DPAs containing Art. 28 obligations are likely to be sufficient to comply with PDPL requirements.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• procedures of data return and disposal; • provisions governing the instructions and communications; and • approvals and notifications required for engaging a sub-processor. Further, the PDPL imposes substantive obligations directly on the processor. **Records of Processing (ROP):** The Regulation introduces detailed procedural, contractual, and documentation requirements for processors. **Sub-processors:** It also regulates the use of sub-processors by requiring prior authorization from the controller and imposing equivalent data protection obligations on any sub-processor. **Cooperation:** It also imposes obligations on processors to assist controllers in responding to data subject requests, complying with regulatory inquiries, and managing personal data breaches. **Data breach:** Processors are also required to notify controllers without undue		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					delay upon becoming aware of a data breach, thereby integrating the processor into the incident response framework. **ROP:** Regulation also introduces record-keeping obligations for processors, obliging them to maintain an internal ROP. However, this is an internal requirement and would not need to be included in the DPA with the controller.		
International data transfers							
24.	**Adequacy decision**	✓	Transfers of personal data from the European Economic Area (EEA) to whitelisted countries[1] subject to an adequacy decision by the European Commission do not have to comply with additional safeguard requirements under the GDPR.	✓	The PDPC is expected to issue a whitelist of countries with adequate personal data protection equivalent to that under the PDPL. Transfer to whitelist countries will not require additional safeguards, e.g., SCCs.	**Minimal difference**	• Monitor for updates from the PDPC on publication of the whitelist and compare against the European Commission's list of adequacy decisions.
25.	**Transfer mechanism**	✓	To transfer personal data from the EEA or the UK to a non-whitelisted jurisdiction, the controller must: • implement an appropriate transfer mechanism (e.g.,	✓	**Cross-Border Data Transfer License** Generally, any cross-border transfer of personal data requires a supplementary license or permit from the PDPC — this is in addition to the main license required for	**Material gaps:** Egypt's cross-border transfer regime is fundamentally different from the GDPR's approach. The practical difficulty with transferring personal data overseas (i.e., obtaining a prior	• Map all cross-border data flows involving personal data subject to the PDPL. • Consider minimizing Egyptian personal data transfers or localizing storage of Egyptian

[1] The European Commission has so far recognized Andorra, Argentina, Brazil, Canada (commercial organizations), the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, Korea, New Zealand, Switzerland, the United Kingdom, and Uruguay as providing adequate protection, as well as the EU-US Data Privacy Framework for relevant transfers to the US.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			standard contractual clauses adopted by the European Commission or the UK equivalent); • carry out a TIA; and • depending on the TIA outcome, implement supplementary measures (e.g., encryption of data in transit and at rest).		all data controllers or processors for any processing activity. This license/permit is granted based on the PDPC's assessment of the adequacy of protection in the destination country, per Article 16 of the Regulations. Cross-border data transfer refers to the transfer, storage, sharing, processing, displaying, using, receiving, retrieving, or granting access and making available (including remote access) to personal data outside of Egypt. Transfers may only be made to jurisdictions specified in the license/permit; and the permit must be updated if additional jurisdictions are added. **Data Transfer Mechanisms** Under Article 14 of the PDPL, cross-border transfer may only occur if the protection level in the foreign country meets or exceeds the requirements under the PDPL. This can be satisfied by transferring data to whitelist countries or by implementing appropriate safeguards. Note that they do not replace the need to obtain	PDPC license/permit for each transfer and updating the license for each additional destination jurisdiction) effectively results in a de facto data localization requirement. The per-jurisdiction licensing and consent requirements represent significant additional compliance burdens not present under the GDPR.	personal data and personal data of residents in Egypt. • Apply for PDPC cross-border transfer supplementary license(s) specifying all destination jurisdictions.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance

					a data transfer license/permit. These mechanisms are merely the means by which an organization may demonstrate to the PDPC as part of the license application that data is being transferred to an "adequate" country.
					• **Whitelist:** transfer personal data to a whitelist country; **or**
					• **Appropriate safeguard:** if the destination country is not on the whitelist, implement appropriate safeguards to ensure adequate protection in the destination countries.
					  ○ These are required as part of the license/permit application — the appropriate safeguard is merely a means to demonstrate adequacy of the destination country if not relying on the whitelist.
					  ○ Appropriate safeguards recognized by the PDPC include the following, although		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					in all cases, such safeguards would remain subject to the PDPC's review and approval as part of the application for the relevant cross-border data transfer license/permit: (1) SCCs (2) BCRs (3) Agreements ensuring equivalent protection, e.g., a DPA **EU SCCs and BCRs** At this stage, as the licensing portal is not yet fully operational and the PDPC has commenced reviewing such applications for local Egyptian entities only, there is no published guidance on how the PDPC will assess or approve these safeguards in practice. Accordingly, it is not currently possible to confirm whether EU SCCs or EU-approved BCRs would, by themselves, satisfy the Egyptian requirements. Greater clarity is expected once the electronic portal of the PDPC becomes fully		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					operational and develops its regulatory practice in this regard. **TIA** A TIA must also be conducted prior to the transfer of data and submitted to the PDPC as part of the cross-border transfer license/permit application. The TIA assesses whether destination countries guarantee sufficient protection under Article 16 of the Regulations, with reference to: • the existence of data protection legislation consistent with the PDPL; • the availability of technical and security measures by the data importer; and • legal rules for compensation in the event of data misuse. Neither the PDPL and Regulations, nor the Guidelines provide a form or minimum level of detail for the TIA. The content is driven by Article 16 of the Regulations: the assessment should address each of the factors listed there in respect of the destination jurisdiction. Accordingly, a proportionate		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					assessment addressing those factors should be sufficient in principle. That said, the TIA is reviewed by the PDPC as part of the license/permit application, and no application has yet been assessed, so we cannot confirm the standard the PDPC will apply in practice.		
Privacy by design / documentary requirements							
26.	**Record of processing (ROP)**	✓	Controllers and processors must maintain records of processing activities containing: • the name and contact details of the controller and, if applicable, the joint controller, the controller's representative, and the DPO; • the purposes of processing; • a description of categories of data subjects and personal data; • the categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or	✓	The PDPL and Regulations require controllers and processors to maintain electronic logs documenting all actions conducted on personal data. This obligation applies on a per-entity basis, i.e., the centralization of a single ROP applying to multiple entities would not be permissible. Such logs must be kept in a clear and retrievable format, enabling the organization to demonstrate compliance with, and to respond effectively to, any law enforcement/ regulatory inquiries or data subject requests. The PDPC also issued the Record of Processing Activities guidelines to	**Manageable gaps:** The PDPL ROP requirements are more granular than Article 30 GDPR. Additional fields include sub-purposes, data owner, data collection source, lawful basis, data hosting environment and location (inside or outside Egypt), data disposal measures, organizational roles with access, legal characterization of recipients, and links to LIAs, DPIAs, TIAs, and data protection agreements. ROPs must be maintained on a per-entity basis (a centralized group-wide ROP is not permissible) and in a clear, retrievable electronic format. The GDPR SME exemption	• Review existing GDPR ROPs against the PDPL controller and processor field requirements and the PDPC Record of Processing Activities Guidelines, and supplement them with the additional PDPL-specific fields. • Prepare a separate ROP for each entity processing Egyptian personal data, rather than relying on a centralized group ROP. • Ensure ROPs are maintained electronically in a clear and retrievable format, and are kept up to date and consistent with the information submitted in the PDPC license/permit application.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			international organizations; • if applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization, and in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards; • if possible, the retention periods and envisaged time limits for the erasure of the different categories of data; and • if possible, a general description of technical and organizational security measures.		provide more detailed guidance. The ROP prepared by controllers must include the following information: • The name and contact details of the controller • The name and contact details of the DPO • The name and contact details of the controller's legal representative • The purpose(s) of processing activity • The sub-purpose(s) of processing, if applicable • The category(ies) of data subjects • The data owner • The categories of personal data, including its classification as non-sensitive data, sensitive data, and children's data • The data collection source • The lawful basis • The legitimate interest assessment link, if applicable • The data hosting environment (on-premises or on-cloud)	(fewer than 250 employees, if processing is likely to pose a risk, isn't occasional, or includes special-category of criminal data) has no equivalent under the PDPL.	

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• The data hosting location (inside or outside Egypt) • The retention period or criteria of determining it • The data disposal measure(s) • The organizational roles with access to the data • The implemented technical security measures • The implemented organizational security measures • The data protection impact assessment link, if applicable • The recipient(s) or category(ies) of recipient(s) • The legal characterization of the recipient(s) • The data protection agreements link (i.e., data processing agreement, data sharing agreement) • The foreign country(ies) data is transferred to • The basis of cross-border transfer • The implemented security measures for cross-border transfer		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• The transfer impact assessment link, if applicable The ROP prepared by processors must include the following information: • The name and contact details of the processor • The name and contact details of the DPO • The name and contact details of the processor's legal representative • The contact details of the controller and the controller's legal representatives and DPO • The data processing agreement link • The retention period and instructions specified by the controller • The data disposal measure(s) • The implemented technical security measures • The implemented organizational security measures • The sub-processor or category(ies) of sub-processor(s)		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					• The sub-processor agreement link • The foreign country(ies) data is transferred to • The legal basis of cross-border transfer of data • The implemented security measures for cross-border transfer of data		
27.	**Data Protection Impact Assessment (DPIA)**	✓	A DPIA should be conducted when a type of processing (particularly using new technologies, and taking into account the nature, scope, context, and purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons.	✓	The PDPL and its Regulations do not contain an express equivalent on conducting DPIAs. However, the Guidelines have provided that controllers and processors are required to conduct a DPIA when the processing is likely to result in a high risk to the individual's rights and freedoms, used to identify, assess, and mitigate the potential data protection risks of that processing. Such DPIA must be properly documented and made available to the PDPC upon request.	**Minimal difference**	N/A
Governance							
28.	**Data Protection Officer (DPO)**	✓	A controller or processor must appoint a DPO if: • the processing is carried out by a public authority or	✓	DPO appointment is mandatory for all controllers and processors under the PDPL and Regulations, regardless of processing type	**Material gaps:** Egypt requires mandatory DPO appointment for all controllers/processors regardless of size or	• Engage local Egyptian counsel as an outsourced DPO (assuming they have passed the DPO's exams and are eligible to act as

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			body, except for courts acting in their judicial capacity; • the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; • the core activities of the controller or the processor consist of processing data on a large scale, of special categories of data, or personal data relating to criminal convictions and offenses; or • where required by Member State law.		or volume. It is a prerequisite for any controller and/or processor to obtain the Main License/Permit. **Foreign DPOs** The DPO may be a foreigner located outside of Egypt, provided that in such case the controller/processor designating the foreigner as DPO must show and confirm that the proposed candidate is readily available to act effectively as point of contact with the PDPC, in accordance with Article 9 (2) of the PDPL, whether through technological means or in-person. Furthermore, the relevant controller/ processor must confirm that there is no overriding obligation, whether in law, treaty, or code of conduct, that prevents the DPO from fully complying with the PDPL as any Egyptian national would. **Qualification Requirements** • Before the DPO is formally appointed, it must register with the PDPC in its DPO Registry by submitting an application to the PDPC, in accordance with Article 8 of the	processing type, whereas the GDPR limits mandatory appointment to defined scenarios. Egypt further requires PDPC registration of DPOs with specific qualification and that have passed the PDPC's exams, which are not required under the GDPR. The obligation to notify PDPC of changes in DPO appointments, ensure uninterrupted DPO coverage, and compile annual reports on the status of privacy protection adds operational complexity.	the organization's outsourced DPO). • Appoint another individual as the DPO and ensure all qualification requirements are satisfied.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					PDPL and Article 8 of its Regulations. • In order to qualify for registration in the DPO Registry, the applicant should possess qualifications and recognized professional certifications corresponding to the category in which the DPO will be registered, undergo and successfully pass the official examinations administered or accredited by the PDPC, and have a clean criminal record. PDPC DPO guidelines specify mandatory qualification, experience, and integrity requirements for DPO registration. **DPO Obligations** • The DPO must perform regular evaluations and inspections of data protection systems, and issue recommendations essential to avoid infringements. They must respond to requests from data subjects, reply to complaints from the PDPC, and take any		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					corrective actions for possible violations. • As part of internal compliance with the PDPL, the DPO should organize necessary training programs for employees. • The DPO has reporting and supervisory duties with the PDPC. It must monitor the application of security policies issued by the PDPC concerning the processing, storage, and circulation of data. An annual report must be submitted to the PDPC on the status of privacy protection. **Termination/Replacement** • Controllers/processors must notify PDPC of any DPO terminations/ replacements and ensure uninterrupted coverage by an approved successor. The PDPC must be notified within 15 days prior to the termination/ replacement's effective date, and such notification must include the reason for termination, the registration code of the newly appointed DPO,		

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					and the duration of the mandate of the newly appointed DPO.		
29.	**Representative**	✓	A controller or processor must appoint a local representative if the controller or processor is not established in the EEA.	✓	Foreign controllers/ processors without a branch or representative office in Egypt must appoint a representative in Egypt through a branch or office acting for or representing them, submitted to and accredited by the PDPC for the license/permit period. If the controller or processor is a natural person, they must appoint an agent within Egypt. The representative acts as a local point of contact and address for service for a foreign entity; this may be performed by a law firm on an outsourced basis, in the same manner as in other jurisdictions. No registration as DPO is required to perform this scope. Where an organization already has a local group entity in Egypt, the local entity may act as the representative office, with its details provided as part of the Main License/Permit application (subject to further PDPC guidance).	**Manageable gaps:** Both frameworks require appointment of a local representative for foreign entities. However, Egypt requires the representative to be accredited by the PDPC for the license/permit period, adding a regulatory oversight layer not present under the GDPR.	• Assess whether a local representative is required (i.e., whether the organization has a branch or representative office in Egypt). • If required, consider engaging local Egyptian counsel as the outsourced local representative or appoint a local branch/office as the representative and obtain PDPC accreditation for the license/permit period. • Submit an application for the approval of the local representative to the PDPC.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
Data subject rights							
30.	**Right to be informed**	✓	Data subjects have the right to be informed about how and why their data is used.	✓	Controllers must provide privacy notices with specified content at or before the time of seeking consent or commencing processing.	**No-action gaps —** See #14 on Privacy Policy Disclosures.	See #14 on Privacy Policy Disclosures.
31.	**Right of access**	✓	Data subjects have the right to request a copy of their personal data from the controller, as well as other relevant information (subject to certain exceptions).	✓	Data subjects have the right to access their personal data held by controllers. Controllers must facilitate the exercise of this right.	**Minimal difference:** Both frameworks recognize a right of access.	• Ensure data subject requests are acknowledged within six working days.
32.	**Right to rectification**	✓	If personal data is inaccurate or incomplete, data subjects have the right to have their data corrected or completed by the controller, without undue delay (subject to certain exceptions).	✓	Data subjects have the right to rectify their personal data.	**Minimal difference:** Both frameworks recognize a right to rectification.	• Ensure data subject requests are acknowledged within six working days.
33.	**Right to erasure**	✓	Data subjects have the right to request that the controller delete their personal data without undue delay (subject to certain exceptions).	✓	Data subjects have the right to erasure of their personal data (subject to certain exceptions).	**Minimal difference:** Both frameworks recognize a right to erasure.	• Ensure data subject requests are acknowledged within six working days.
34.	**Right to object/restrict processing**	✓	Data subjects have the right to object to, or request that the controller restricts, processing in certain circumstances.	✓	Data subjects have the right to object to and require the cessation of the processing of their personal data. Further, data subjects have the right to request the temporary restriction of the	**Minimal difference:** Both frameworks recognize a right to object and restrict processing.	• Ensure data subject requests are acknowledged within six working days.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
					processing of their personal data.		
35.	**Right to data portability**	✓	Data subjects have the right to request that their personal data be transmitted to another controller (subject to certain exceptions).	✓	Data subjects have the right to request the transfer of their personal data from a controller/processor to another, in a structured, commonly used, and machine-readable format.	**Minimal difference:** Both frameworks recognize a right to data portability.	• Ensure data subject requests are acknowledged within six working days.
36.	**Right not to be subject to automated decision-making**	✓	Data subjects have the right not to be subject to a decision based solely on automated processing (i.e., processing carried out without human intervention that has a legal or similarly significant effect on the data subject).	✗	The PDPL, Regulations, and Guidelines do not contain an express right not to be subject to automated decision-making.	**No-action gap:** The PDPL, Regulations, and Guidelines do not provide for the right not to be subject to automated decision-making.	N/A
37.	**Right to withdraw consent**	✓	Data subjects have the right to withdraw their consent to the processing, if such consent is relied on as the legal basis for processing (it must be as easy to withdraw as to give consent).	✓	Data subjects have the right to withdraw consent. Consent records must include the withdrawal details, date, and time. In the DEM context, refusal/withdrawal must be available through PDPC-approved methods. Personal data must be permanently erased upon receipt of the consent withdrawal, where applicable.	**Manageable gaps:** Both frameworks recognize the right to withdraw consent. Egypt adds requirements for PDPC-approved withdrawal methods (particularly for marketing) and mandatory recording of withdrawal details. The mandatory erasure upon withdrawal in the marketing context exceeds standard GDPR practice.	• Ensure withdrawal mechanisms are available through PDPC-approved methods, including direct messages via social media platforms, SMS, electronic mail, telephone calls, or any other approved technological means. • Record consent withdrawal details (date, time, method) in a consent register. • Ensure data subject requests are acknowledged within six working days.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
38.	**Right to lodge complaint with regulator**	✓	Data subjects have a right to lodge a complaint with the relevant data protection authority.	✓	Data subjects have the right to lodge a complaint with the PDPC. Privacy notices must include information about this right and the process for exercising it.	**Minimal difference:** Both frameworks provide for complaints to the supervisory authority. Egypt requires privacy notices to specify the PDPC complaint process.	• Ensure privacy policy includes contact details of the PDPC and methods of exercising this right.
39.	**Breach notification to regulator**	✓	**Threshold** Personal data breaches that are likely to result in a risk to the rights and freedoms of natural persons must be notified. **Notification Content** The notification to the relevant data protection authority should include: • categories and approximate number of data subjects; • the nature of the data breach; • the name and contact details of the DPO; • the likely consequences of the data breach; and • the measures taken, or proposed to be taken, by the controller to address the data breach, and measures to mitigate its possible adverse effects.	✓	**Threshold** All personal data breach notifications have no materiality threshold. This means that technically all personal data breaches, no matter how small (including those that do not pose any material harm to data subjects), need to be notified. **Notification Timing** • Organizations must notify the PDPC **within 72 hours** of becoming aware of a personal data breach. • Notifications must be submitted through secure PDPC channels (electronic portal/hotline once designated). • Each incident must be recorded in a centralized electronic register with timestamps of discovery and notification.	**Material gaps:** While both frameworks require notification within 72 hours, Egypt has no materiality threshold (all breaches must be reported, regardless of risk level). This is a stricter and more expansive obligation than the GDPR's risk-based approach.	• Update internal incident response policy for PDPL notification requirements. • Use PDPC notification templates.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			Notification Timing Relevant data protection authorities should be notified **without undue delay and no later than 72 hours** after becoming aware of the breach, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons.		• If the breach relates to national security, enhanced notification obligations require identification of the nexus and estimates of the data volume and potential harm. Organizations must notify the PDPC **immediately** upon becoming aware of a personal data breach. • The Egyptian Anti-Cybercrime Law No. 175 of 2018 separately requires **immediate** notification to the Egyptian CERT for data/cybersecurity breaches linked to unauthorized access/interception of service provider systems that compromise user data.		
40.	**Notification to affected data subjects**	✓	**Threshold** Personal data breaches that are likely to result in a high risk to the rights and freedoms of the natural person must be notified. **Timing** Notification should be made to affected data	✓	**Threshold** There is no materiality threshold — all breached data subjects must be notified. **Timing** Data subjects must be notified **within three**	**Material gaps:** Egypt requires notification for all breaches (no materiality threshold) within three business days after the PDPC notification. This is a stricter and more expansive obligation	• Update internal incident response policy for PDPL notification requirements. • Use notification templates prepared by PDPC.

	Issue	Does the GDPR cover this issue?	Scope	Does the PDPL or Regulation cover this issue?	Scope	Key gaps	Potential step(s) for PDPL compliance
			subjects **without undue delay** only if a breach is likely to result in a high risk to the rights and freedoms of the affected individuals.		**business days** after notifying the PDPC. The PDPC provides templates for data subject notifications.	than the GDPR's risk-based approach.	

Conclusion

With the Regulations now issued and the grace period having expired on October 31, 2026, entities subject to the PDPL should take steps now to bring their privacy programs in line with the new framework. We recommend the following key actions:

- **Appoint a DPO first.** Identify a suitably certified DPO and register them with the PDPC. This should be a priority, as a DPO must be in place before any license or permit can be obtained.
- **Conduct a gap assessment.** Review your current privacy program against the PDPL and the Regulations to identify any compliance gaps.
- **Map your data.** Map the personal data you control or process and how it flows through the business, classify it, and confirm there is an appropriate legal basis under the PDPL for each use.
- **Update key documents and safeguards.** Review and update, among other things, privacy policies, electronic logs (such as records of processing (ROP)), agreements with third-party processors and controllers, and the safeguards in place for cross-border data transfers.
- **Prepare for licensing.** Gather the documents and information the PDPC requires for license and permit applications. The PDPC's online application portal is currently only partially operational and is available only to local Egyptian entities, so foreign entities should apply offline and complete the process in person through their duly appointed legal representatives.
- **Engage early with the PDPC.** Start the licensing and DPO registration processes and/or contact the PDPC to show your willingness to comply. Demonstrating this proactive approach may help reduce future compliance and enforcement risk.

Contacts



Calum Docherty
Partner
calum.docherty@lw.com
+44.20.7710.1079
London



Rhys McWhirter
Partner
rhys.mcwhirter@lw.com
+852.2912.2686
Hong Kong



Esther Franks
Counsel
esther.franks@lw.com
+65.6437.5345
Singapore



Danielle van der Merwe
Counsel
danielle.vandermerwe@lw.com
+971.4.704.6351
Dubai / London



Hayley M. Pizzey
Counsel
hayley.pizzey@lw.com
+44.20.7710.1005
London



Bianca H. Lee
Associate
bianca.lee@lw.com
+852.2912.2500
Hong Kong



Amy Smyth
Knowledge Management Counsel
amy.smyth@lw.com
+44.20.7710.4772
London

The authors would like to thank **Ernest Lok** for his contribution to this report.

The authors would like to thank **Mohamed Hashish** (Managing Partner) and **Mariam Rabie** (Associate) at **Soliman**, **Hashish & Partners**, who provided the Egyptian law input for this report, for their contribution.

Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company, in South Korea as a Foreign Legal Consultant Office, and in Saudi Arabia through a limited liability company. © Copyright 2026 Latham & Watkins. All Rights Reserved.