International Comparative Legal Guides

Data Protection 2026

A practical cross-border resource to inform legal minds

13th Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

glg Global Legal Group

iclg

Expert Analysis Chapters

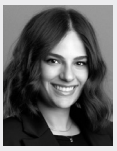
Q&A Chapters

Egypt


Dr. Ibrahim Shehata


Hesham Kamel


Mohamed Abed


Safa Rabea

Shehata & Partners Law Firm

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Law No. 151 of 2020 ("**PDPL**") and its executive regulations issued by the Minister of Communications and Information Technology Decree No. 816 of 2025 ("**Regulations**") constitute the principal data protection legislation in Egypt, focusing on safeguarding the privacy and data rights of individuals and entities.

1.2 Is there any other general legislation that impacts data protection?

Egypt's data protection framework is influenced by several pieces of general legislation that provide legal safeguards for individual privacy and data security:

1. **Constitutional protection of privacy**
   Privacy is a fundamental right enshrined in the 2014 Egyptian Constitution, which provides comprehensive legal protection for individuals. The relevant articles are:
   - Article 28, stipulating that information-based activities are key components of the national economy, and that the State commits to protecting them and increasing their competitiveness.
   - Article 31, stipulating that the security of the information space is an integral part of the national economy and security system.
   - Article 57, explicitly stating that "private life is inviolable, safeguarded, and may not be infringed upon", ensuring protection against unlawful searches, seizures and bodily harm, as well as unauthorised entry, surveillance or interference in family relationships. The Constitution also guarantees the confidentiality of personal communications, including letters, emails, phone calls and electronic correspondence, prohibiting unauthorised collection, use or disclosure of personal data.
   - Additionally, Article 57 reinforces the inviolability of communication channels, safeguarding them from interception or unlawful access.
2. **Telecommunications data protection**
   The Telecommunications Law No. 10 of 2003 introduces additional sector-specific protections, as it requires licensed operators to maintain the confidentiality of private communications and calls.
3. **Cybercrimes Law**
   The Cybercrimes Law No. 175 of 2018 establishes data privacy safeguards by regulating online activities and penalising unauthorised access to personal data and IT systems.
   Telecommunications and information technology service providers are mandated to store user data for 180 days, maintain its confidentiality, and refrain from disclosing it without a judicial order. Additionally, they must implement security measures, such as encryption and multi-factor authentication.
4. **Electronic signature and IT security**
   The Electronic Signature Law No. 15 of 2004 mandates that electronic signature data, electronic media and information submitted by a licensed certification authority are considered confidential.
   Those who access or handle such information as part of their work are prohibited from disclosing it to third parties or using it for any purpose other than the one for which it was provided.
   Additionally, the executive regulations of this law require applicants for e-signature services to implement systems that ensure the security and confidentiality of information, aligning with legal standards.
5. **Criminal law protections**
   The Penalties Law No. 58 of 1937 criminalises the invasion of privacy and the unauthorised collection, use or disclosure of personal information. It imposes penalties on individuals or entities that unlawfully access, obtain or share personal data without legal justification, reinforcing data privacy protections under Egyptian law.

1.3 Is there any sector-specific legislation that impacts data protection?

While the PDPL provides a comprehensive legal framework for safeguarding personal information, the Telecommunications Law No. 10 of 2003 introduces sector-specific obligations that apply to the telecommunications and information technology sector.

Furthermore, the banking sector is excluded from the scope of application of the PDPL. Therefore, it remains subject to the instructions of the Central Bank of Egypt.

1.4 What authority(ies) are responsible for data protection?

The Personal Data Protection Centre ("**Centre**") is the competent authority for implementing the PDPL.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**
  Any data related to an identified or identifiable natural person, either directly or indirectly, through linking such personal data with any other data, such as name, voice, image, identification number, online identifier, or any data that determines the psychological, medical, economic, cultural or social identity of a natural person.
- **"Processing"**
  Any electronic or technical process for writing, collecting, recording, storing, preserving, merging, displaying, sending, receiving, circulating, publishing, erasing, altering, modifying, retrieving or analysing personal data using any medium, device or electronic or technical means, whether performed partially or entirely.
- **"Controller"**
  Any natural or legal person who, by the nature of their work, has the right to obtain personal data, determine the method, manner and criteria for its retention, processing and control, in accordance with the specified purpose of their activity.
- **"Processor"**
  Any natural or legal person who, by the nature of their work, is specialised in processing personal data for their own benefit or on behalf of the controller, in accordance with the controller's instructions and the agreement concluded with them.
- **"Data Subject"**
  Any natural person to whom electronically processed personal data pertains, either legally or in practice, and who can be identified or distinguished from others.
- **"Sensitive Personal Data"/"Special Categories of Personal Data"**
  Data that discloses mental, psychological, physical or genetic health, biometric data, financial data, religious beliefs, political opinions or criminal status. In all cases, children's data is considered sensitive personal data.
- **"Data Breach"**
  Any unauthorised access to personal data or unlawful access to it, or any illegal process of copying, sending, distributing, exchanging, transferring or circulating aimed at revealing or disclosing personal data, or destroying, modifying or altering it during its storage, transmission or processing.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL has an extra-territorial effect and may apply to businesses established outside Egypt under certain circumstances. Its extra-territorial effect is structured around the commission of one of the offences set out therein, if the offender is:

- an Egyptian business, regardless of whether the offence occurs inside or outside Egypt;
- a non-Egyptian business residing in Egypt; or
- a non-Egyptian business located outside Egypt, provided that:
  - the act is punishable under the laws of the country in which it occurred; and
  - the personal data subject to the offence relates to Egyptian nationals, or foreign nationals residing in Egypt.

Accordingly, a business established in another jurisdiction may be subject to the PDPL if it processes personal data related to individuals residing in Egypt and the underlying activity constitutes an offence under both Egyptian law and the law of the country where the activity took place.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The following types of data are excluded from the material scope of the PDPL:

- Data processed by a person for personal use.
- Data processed for media purposes, as long as it is truthful, accurate and complies with media laws.
- Data processed for official statistical purposes.
- Data related to legal investigations, inquiries and court proceedings.
- Data held by national security authorities.
- Data held by the Central Bank of Egypt and the entities falling under its supervision, except for money transfer and currency exchange companies.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

Based on the provisions of the PDPL and the current guidelines of the Centre, the key principles are as follows:

- **Transparency**
  Personal data must be processed in a manner that is transparent, clear and honest towards the data subject. Accordingly, the PDPL requires the data user (controller or processor) to declare the processing purposes to the data subject.
- **Lawful basis for processing**
  To lawfully process personal data, data users must rely on at least one of the legal bases enumerated by Article 6 of the PDPL: data subject's consent; fulfilment of a legal obligation; fulfilment of a contractual obligation; legitimate interest; the defence of a legal claim or right; and the execution of court judgments or orders issued by competent investigative authorities.
- **Purpose limitation**
  The purpose refers to the reason or objective for which personal data is collected and processed, defining the scope and limitations of the processing activity. This reflects the requirement that personal data must be processed for specific purposes.
- **Data minimisation**
  Personal data must be collected and processed only to the extent that is relevant, adequate and necessary in relation to the intended purposes. This places an obligation on the controller to verify the adequacy of the data collected.

- **Proportionality**
  Any processing of personal data must be appropriate and not excessive in relation to the purposes for which it is collected. This means that a data user must ensure that the scope, volume and impact of data processing are proportionate to the intended and declared purpose.
- **Retention**
  The PDPL requires data users to specify a retention period for the personal data they collect. Once this period expires, the data must be erased, or anonymised where retention is justified by legal or national security considerations.
- **Accuracy**
  Personal data must be accurate, complete and kept up-to-date, in line with the purposes of the processing activity.
- **Accountability**
  Appropriate technical and organisational measures must be implemented to ensure that personal data is processed in compliance with all data protection principles and obligations. Furthermore, compliance must be demonstrable through appropriate documentation, in accordance with the data protection regulatory framework.
- **Fairness**
  Personal data should be processed in a manner that aligns with data subjects' reasonable expectations and ensures that they do not suffer any unjustifiable harm. While this is not explicitly mentioned in a standalone provision under the PDPL or the regulations, it may result from the requirement of processing data in a 'suitable' manner, for legitimate and specified purposes.
- **Storage limitation**
  Personal data must not be retained for longer than necessary to achieve the purposes of the processing activity.
- **Data security**
  Personal data must be secured throughout its entire lifecycle against unlawful or unauthorised processing, access, alteration, damage, loss or destruction.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
  Data subjects have the right to be informed of the personal data held about them by any data user. This includes the right to access and obtain a copy of their data, as well as information regarding the nature, purpose and scope of its processing.
- **Right to rectification of errors**
  Data subjects have the right to request the correction, amendment, updating or completion of inaccurate or incomplete personal data held by the data user.
- **Right to deletion/right to be forgotten**
  Data subjects may request the deletion of their personal data. Additionally, controllers are required to delete data collected upon the completion of the initial purpose for which the personal data was collected.
- **Right to object to processing**
  Data subjects have the right to object to the collection, processing, disclosure or dissemination of their personal data without their explicit consent, except where such processing is authorised by law.
- **Right to restrict processing**
  Data subjects have the right to restrict processing within a defined scope and purpose.
- **Right to data portability**
  The PDPL does not expressly include the right to data portability.
- **Right to withdraw consent**
  Data subjects may withdraw their consent at any time. Upon withdrawal, the data user must cease all processing activities related to that data, unless a legal obligation or overriding legitimate interest justifies continued processing.
- **Right to object to marketing**
  The PDPL prohibits any electronic communication for the purpose of direct marketing to the data subject, unless they provided their consent.
- **Right to protection against solely automated decision-making and profiling**
  While the PDPL does not explicitly grant this specific right, a data subject has the right to object to how their data is being processed or to the results of such processing where such processing violates their fundamental rights and liberties.
- **Right to complain to the relevant data protection authority(ies)**
  Without prejudice to the right to seek judicial remedies, data subjects may file a complaint with the Centre in cases where their rights have been violated or infringed, where they have not been able to exercise their rights, or where they object to decisions issued by the data protection officer ("**DPO**") of the data user in relation to their submitted requests.
- **Right to compensation**
  Data subjects have the right to claim compensation for any material or moral damage resulting from the unlawful processing or misuse of their personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Data subjects do not have the right to mandate not-for-profit organisations to seek remedies on their behalf or to seek collective redress. Alternatively, data subjects may do the following:

- **Multiple claimants in a single action**: Under the civil and commercial procedures law, multiple claimants may bring a single action where the subject matter or legal cause is common or closely connected. Each claimant must individually establish standing, damage and causation. However, this mechanism does not constitute collective redress in the technical sense.
- **Regulatory complaints**: In data protection matters, data subjects may file complaints with the Centre. The Centre's decisions are administrative in nature and do not amount to judicial collective redress or collective compensation.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The PDPL imposes additional obligations in relation to the processing of children's data, as follows:

- If the child is under 15 years old, valid explicit consent must be obtained from the child's guardian in writing. Such consent must be limited in time and may subsequently be withdrawn.
- If the child is at least 15 years old, the child, or their guardian, must give their written consent.
- Where a child participates in a game or competition, the requested data must be limited to what is strictly necessary. Moreover, such data may not subsequently be used in any operations involving profiling, tracking or behavioural monitoring of children.

Furthermore, it is prohibited to use children's data for any tracking, surveillance or behavioural monitoring purposes whenever such data is obtained due to the child's participation in a game, competition or any other activity.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the PDPL, businesses engaged in the processing of personal data are legally required to obtain a licence or permit from the Centre prior to commencing processing activities. This applies to data users and to entities engaged in processing sensitive personal data or carrying out cross-border transfers of personal data.

The PDPL further requires that businesses maintain internal records of processing operations, appoint a DPO, and cooperate with the inspections carried out by the Centre.

Failure to obtain the appropriate authorisation or comply with registration obligations may result in administrative fines or criminal penalties.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registration and licensing framework is designed to be specific and structured, rather than general. The PDPL makes it clear that the Centre is responsible for issuing various types of licences, permits and accreditations based on the nature of the processing activity.

These include licences/permits to act as a controller, processor or both, to carry out cross-border transfers of data, to use visual surveillance tools (i.e., CCTV), and to conduct electronic direct marketing ("**EDM**").

The Regulations further define the categories, procedures, conditions, levels and forms associated with each type of licence or permit. Depending on the nature of the organisation's activities, the Centre may impose additional requirements.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Any individual or entity acting as a controller or processor, regardless of the volume of data processed or the purpose of processing, must obtain the required licence or permit from the Centre before carrying out any processing of personal data.

However, this does not apply to sectors excluded from the PDPL's scope of application, as discussed in question 3.2.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to our answer to question 7.3.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

An application for a licence or permit must include certain information demonstrating the applicant's compliance with the data protection framework. This generally includes: the mechanisms used to obtain the data subject's consent and enable the exercise of their legal rights; the technical and organisational measures adopted to secure and protect personal data in accordance with the standards issued by the Centre; and confirmation of compliance with the PDPL and the relevant licensing conditions, enabling the Centre to exercise supervision and inspection.

For legal entities, the application must also include evidence of maintaining the required electronic records, documentation evidencing the appointment of a DPO and their independence in performing their duties, and confirmation of compliance with the rules governing the processing of sensitive personal data and children's data.

7.6 What are the sanctions for failure to register/notify where required?

Failure to obtain the required licences or permits from the Centre prior to processing personal data may expose the data user to criminal penalties under the PDPL, including a fine ranging from EGP 500,000 to EGP 5 million.

7.7 What is the fee per registration/notification (if applicable)?

Fees vary depending on whether the entity obtains a licence for ongoing processing or a permit for a specific and temporary purpose, to conduct the activities of a controller, processor, or both, and the volume of personal data records processed.

For a licence that allows the undertaking of the activities of both a controller and processor, which is granted for three years, the annual fees range from no fee for processing up to 100,000 records, to a maximum of EGP 2 million for processing volumes exceeding 5 million records. Where the licence is granted to conduct either controller or processor activities, the applicable fees are 50% less than the prescribed amount for a collective licence.

For a permit that allows the undertaking of the activities of both a controller and processor, which may be granted for periods of up to one year, the fees depend on both the duration of the permit and the number of personal data records

processed. Processing up to 25,000 records is exempt from fees, while higher volumes may incur fees ranging from EGP 10,000 up to EGP 500,000, depending on the number of records and the permit duration. Where the permit is granted to conduct either controller or processor activities, the applicable fees are 50% less than the prescribed amount for a collective permit.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

A licence renewal request must be submitted to the Centre at least three months before its expiry.

A permit renewal request must be submitted at least one month before its expiry.

Both licences and permits may be renewed multiple times.

7.9 Is any prior approval required from the data protection regulator?

The PDPL requires prior approval from the Centre before carrying out certain personal data processing activities. Thus, data users must obtain licences or permits for:

- Data retention, processing and handling activities.
- Cross-border transfers of personal data.
- EDM.
- Processing of sensitive personal data.
- Use of visual surveillance tools in public spaces.
- Processing carried out by associations, unions or clubs concerning their members' data.

The Centre evaluates licence or permit applications in accordance with the procedures outlined in the Regulations, and may require additional guarantees or supporting documents.

7.10 Can the registration/notification be completed online?

As of April 2026, the Centre has not yet implemented the electronic registration system on its website. However, the Regulations require the establishment of an interactive platform for registration and licensing procedures, which is expected to be launched before 31 October 2026, the date when the grace periods ends.

7.11 Is there a publicly available list of completed registrations/notifications?

As of April 2026, the registration/notification process has not yet started. Therefore, there is currently no publicly available list of completed registrations/notifications.

7.12 How long does a typical registration/notification process take?

As of April 2026, the registration/notification process has not yet started. However, the Regulations stipulate that the Centre has 90 days to process an application, provided that it contains all the required information and documents. If the Centre does not respond within this period, the application is deemed rejected.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO is mandatory for all legal entities acting as controllers or processors.

For individuals, they are personally responsible for complying with the PDPL's provisions.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Legal representatives of entities failing to appoint a DPO are sanctioned with a fine ranging from EGP 200,000 to EGP 2 million.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The Regulations provide that controllers and processors applying for permits or licences must provide an acknowledgement that they will give the DPO the necessary independence in undertaking their responsibilities. However, neither the PDPL nor the Regulations contain any explicit protections from disciplinary measures or other employment consequences.

If the contract with the DPO is terminated, a data user must notify the Centre at least 15 days before the date of termination, and indicate the replacement, without any obligation to provide any justifications.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A DPO may serve multiple unrelated entities, provided that all parties agree and no conflicts of interest arise, subject to the Centre's approval.

A DPO may also serve a group of related entities that complement one another through data sharing, provided the Centre is duly notified.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The general qualifications that apply to DPOs are as follows:

- The applicant must hold relevant academic qualifications or professional certifications and possess practical experience in related fields, in accordance with the standards approved by the Centre.
- The applicant must pass the examinations approved by the Centre, taking into account the nature and scale of the personal data processing activities subject to the registration request.
- The applicant must not have been previously convicted of any crimes involving dishonesty or breach of trust.

Based on the DPO's qualifications and level of experience, a DPO may fall under one of the following categories:

- **Category A (Lead DPO)**: This category allows a DPO to oversee more than 2 million personal data records, with no upper limit. DPOs in this category may serve telecommunications operators, major hospitals, ride-hailing and transport platforms, and large insurance companies.
- **Category B (Advanced DPO)**: This category allows a DPO to oversee up to 2 million personal data records. DPOs in this category may serve schools and universities, HR and recruitment firms, medium-sized e-commerce platforms, transportation companies and fitness chains.
- **Category C (Entry-Level DPO)**: This category allows a DPO to oversee up to 100,000 personal data records. DPOs in this category may serve retail stores (non-chain), cafés, restaurants, salons, fitness centres, photography studios and small travel agencies.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO's main responsibilities include:

- Conducting periodic assessments and audits of personal data protection systems, documenting the results and issuing recommendations to enhance data protection.
- Acting as a direct point of contact with the Centre and implementing its decisions.
- Enabling data subjects to exercise their rights under the PDPL.
- Notifying the Centre in the event of any personal data breach or violation.
- Responding to requests submitted by data subjects or other concerned parties, as well as responding to complaints submitted to the Centre.
- Maintaining and updating the personal data register.
- Addressing any violations related to personal data and taking corrective actions.
- Organising training programmes for employees to ensure awareness and compliance with data protection requirements.
- Monitoring the implementation of security policies issued by the Centre and submitting an annual report on the status of privacy protection within the data user's structure.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the appointment and replacement of a DPO must be notified to the Centre, subject to its registration requirements.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

While the PDPL and the Regulations do not contain such an obligation, the Centre requires, through its guidelines, that the contact details of the DPO be included in the privacy notice.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

It is not explicitly mandatory under the PDPL to conclude a written agreement between a controller and a processor. However, a processor is required to act on the written instructions of the controller, which may amount in practice to a written contract. Further, the PDPL stipulates that it is the controller's responsibility to set the methods and criteria for processing, unless this task is delegated to the processor under a written agreement.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Please refer to our answer to question 9.1.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

EDM is broadly defined under the PDPL as the sending, by any technological means, of any messages, statements, advertisements or marketing content that directly or indirectly promotes goods, services, or commercial, political, social or charitable requests, targeted at specific individuals.

Accordingly, the means through which EDM is carried out encompass all forms of communication undertaken through technological means, including emails, text messages (SMS or instant messaging), live telephone calls and automated calls.

The obligations and restrictions are as follows:

- **For creators (those who determine the purposes and means of the EDM)**:
  - Obtaining an EDM licence or permit titled "EDM for self" prior to initiating any related activities.
  - Obtaining the data subject's valid consent in advance.
  - Executing opt-out requests without undue delay.
  - Maintaining an updated and accurate record of all opt-out requests.
- **For senders (those who are responsible for delivering the EDM communications)**:
  - Obtaining an EDM licence or permit titled "EDM for others" prior to sending any EDM communications.
  - Ensuring that the data subject's valid consent is obtained.
  - Refraining from disclosing the data subject's contact details to any unauthorised entity.
  - Maintaining electronic records evidencing the data subject's consent, including any amendments to, or withdrawal of, consent. Such records must be retained for a period of three years from the date of the last communication sent to the data subject.

- **Regarding the content of the EDM communications, they should contain the following elements**:
  - The identity of both the creator and the sender.
  - The contact details of the sender.
  - The purpose of the EDM in explicit terms.
  - A valid opt-out mechanism.

During the grace period ending on 31 October 2026, creators may rely on the "soft opt-in" mechanism to lawfully continue sending EDM communications to existing customers, as per the Centre's guidelines. This is to ease their compliance efforts during this period.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The PDPL does not explicitly distinguish between business-to-consumer ("**B2C**") and business-to-business ("**B2B**") contexts. The restrictions on EDM apply broadly to any processing of personal data, including contact information used for marketing purposes. Therefore, if a B2B marketing communication involves the use of personal data that allows for the identification of a data subject (e.g., a named employee's email or phone number), the same requirements mentioned under question 10.1 would apply.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to our answer to question 10.1.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The PDPL does not provide an explicit answer to this issue. However, if a data user falls within the scope of application of the PDPL, as discussed in question 3.1, then EDM sent from other jurisdictions may also be subject to the same requirements discussed in question 10.1.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Centre is responsible for issuing the required licences and permits to undertake EDM activities, overseeing their compliance with the PDPL, and receiving data subjects' complaints.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

It is lawful to purchase marketing lists from third parties. However, creators (as defined in question 10.1) are legally required to ascertain the existence of a valid lawful basis before using or reusing third-party data. Such measures include:

- Carrying out due diligence on the chain of collection.
- Verifying the lawful basis on which data is collected.
- Ensuring that data subjects were informed that their data could be used by third parties.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sending EDM communications in breach of the PDPL is sanctioned by a fine ranging from EGP 200,000 to EGP 2 million.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The use of cookies or similar tracking technologies for EDM purposes is subject to the same obligations discussed in question 10.1.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Centre published EDM guidelines as part of its mandate to spread awareness among data users. Moreover, it explicitly allowed creators to rely on the "soft opt-in" mechanism during the grace period, ending on 31 October 2026.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The same penalties as discussed in question 10.7.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The PDPL adopts a broad concept of transfer, which covers any transfer, storage, sharing, disclosure, or making available of personal data, whether for processing, storage or any other purpose. In this regard, the key requirements are as follows:

- The controller or processor must obtain a licence or permit from the Centre, based on its assessment of the adequacy of the level of protection in the destination country.
- Personal data may only be transferred to the country or countries specified in the licence or permit, and any addition of new countries requires an update of such licence/permit.
- The controller or processor must obtain the consent of the data subject for the cross-border transfer.
- The transfer, storage or sharing of personal data outside Egypt should be made to a destination country that ensures a level of data protection not less than the level prescribed under the PDPL.
- Notwithstanding the adequacy of the level of protection requirement, cross-border transfers to countries

that do not provide an equivalent level of protection may be permitted subject to the explicit consent of the data subject (or their representative), and only in limited cases, as discussed in question 12.2.

- Appropriate technical and organisational measures must be implemented to ensure an adequate level of protection for personal data during transfer, storage or sharing, in line with the scope and nature of the data and the terms of the licence or permit.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses are required to obtain a licence or a permit prior to transferring personal data abroad, provided that the destination country has a level of protection equivalent to the PDPL.

A data transfer may occur to a country that does not have a level of protection equivalent to the PDPL, provided that (i) the data subject concerned has given explicit consent, and (ii) pursuant to the following situations:

- Protecting the life of the data subject and providing medical care, treatment or health services management.
- Fulfilling obligations necessary to establish, exercise or defend a right before judicial authorities.
- Concluding or performing a contract between the controller and a third party for the benefit of the data subject.
- Taking measures related to international judicial cooperation, or where necessary or legally required to protect the public interest.
- Making monetary transfers to another country in accordance with its applicable laws.
- Where the transfer or processing is carried out pursuant to a bilateral or multilateral international agreement to which Egypt is a party.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Please refer to our answer to question 12.1.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

It is up to the Centre to assess whether a given country provides an adequate level of protection.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

No guidance has been issued.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

No guidance has been issued.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Egyptian law does not regulate whistleblower protection.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Egyptian law does not regulate whistleblower protection.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Yes, the use of CCTV or other video surveillance systems installed in public areas is subject to a special permit or licence. Further, there must be a visible public notice to inform individuals of the presence and operation of visual surveillance tools.

14.2 Are there limits on the purposes for which CCTV data may be used?

No, there are not.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There is no specific or settled guidance directly addressing the monitoring of employees. However, the existence of an employer–employee relationship does not remove the employee's right to privacy. Employers act as data controllers and may process employee personal data only for lawful, specific and legitimate purposes, and only to the extent necessary and proportionate, in accordance with the PDPL.

Moreover, employee monitoring, including time tracking and attendance systems, may be permitted where it is necessary for work organisation, wage calculation or legal compliance, provided employees are informed and provide their consent in advance. Hidden, excessive or continuous monitoring may be prohibited, as it could violate the principle of necessity under the PDPL.

Furthermore, remote work does not necessarily expand the employer's monitoring powers. Employers may monitor working hours or performance only to the extent required to perform the employment contract. Intrusive monitoring, constant surveillance or the use of cameras in the employee's home is not permitted, as it interferes with the employee's constitutionally protected private life and exceeds what is necessary under the PDPL.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Processing employees' personal data requires a valid lawful basis. Although consent may in some cases serve as that basis, it is often not the most appropriate basis in the employment context, given the imbalance in the employer–employee relationship and the resulting doubts as to whether consent can be freely given or withdrawn. Employers should therefore consider relying on other lawful bases, such as the performance of the employment contract, compliance with legal obligations, or the employer's legitimate interests, where applicable and subject to the relevant legal safeguards.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

No such requirement exists under Egyptian law.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Please refer to our answer to question 15.1.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Both controllers and processors are required to ensure the security of personal data. Furthermore, to obtain a permit or licence to undertake the activities of a controller, processor or both, the applicant must indicate the security measures that they will implement.

However, the scope of their respective obligations differs. A controller is required to take all the technical and regulatory measures, and apply all necessary standards, to protect personal data and keep it secure, in order to preserve its confidentiality and integrity.

A processor, on the other hand, must protect and secure its processing activities, the media and the electronic devices used in this regard, as well as the personal data itself.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe.

If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Data breaches must be notified to the Centre within 72 hours of the controller or processor becoming aware of the breach. Where the breach relates to national security considerations, notification must be made without delay.

Notifications must be submitted through the designated channels and recorded in a secure breach register, and must include details of the breach, affected data, potential impact, mitigation measures and the DPO's details.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Affected data subjects must be notified within three working days of notifying the Centre, with information on the breach and the measures taken.

16.4 What are the maximum penalties for personal data security breaches?

A controller or processor who fails to implement appropriate security measures or to notify the Centre of data breaches may be subject to a fine ranging from EGP 300,000 to EGP 3 million. Administrative sanctions may also be imposed by the Centre.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative powers**: The Centre is empowered to receive and examine complaints concerning violations of the PDPL, issue decisions in relation to such complaints, supervise and inspect individuals and entities subject to its provisions, and take the necessary legal measures.

(b) **Corrective powers**: The Centre is empowered to take appropriate corrective measures in the event of violations of the PDPL, including ordering the offending party to cease the infringing activity and to remedy its causes and consequences within a specified period. The Centre may also suspend a DPO where they fail to meet the conditions of their registration, require their replacement, and oblige the concerned entity to appoint an alternative DPO from among those registered with the Centre within a prescribed timeframe.

(c) **Authorisation and advisory powers**: The Centre is the competent authority to issue permits, licences and accreditations. It is also tasked with coordinating and collaborating with all governmental and non-governmental entities to ensure the adoption of data protection measures. The Centre may also give its opinion on draft legislation and international treaties related to personal data.

(d) **Imposition of administrative fines for infringements of specified legal provisions**: The Centre is empowered to impose administrative sanctions. This may begin with the issuance of a warning to the person found to be in violation of the PDPL, requiring them to comply with its provisions within a specified period. If this duration lapses without compliance with the PDPL, the Centre may issue another warning, suspend or revoke the licence/permit, and place the person concerned under enhanced scrutiny.

(e) **Non-compliance with a data protection authority**: Non-compliance may result in administrative sanctions, as well as criminal sanctions, including fines and imprisonment.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Centre has the power to regulate all types of processing activities. However, it does not have the power to ban any of them.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As the Centre was only recently established, there are not yet any published cases from which a reliable answer can be drawn.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

As the Centre was only recently established, there are not yet any published cases from which a reliable answer can be drawn.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In Egypt, businesses do not typically respond to foreign e-discovery requests in the same manner as parties in common-law jurisdictions. Egyptian procedural law does not recognise a general discovery or disclosure process, so a foreign subpoena or disclosure demand would not usually be complied with solely because it was issued abroad.

In practice, the recipient would normally take the advice of a legal counsel, verify whether the request has been brought through a recognised judicial assistance channel, and assess whether there is a valid basis under Egyptian law to disclose the requested material.

Where personal data is involved, a foreign e-discovery request, or request for disclosure from foreign law enforcement agencies, might fall under the restrictions discussed in section 12, as it is considered a cross-border transfer of personal data.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There is no guidance in this regard.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Automated decision-making involving the processing of personal data using artificial intelligence is subject to the same general requirements of processing. Accordingly, there must be a lawful basis for conducting such processing, such as consent or the execution of a contract.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

There is no guidance in this regard.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The most significant development has been the issuance and entry into force of the Regulations in November 2025, which triggered the grace period ending on 31 October 2026 and clarified many practical aspects of the PDPL.

Furthermore, in September 2025, prior to the issuance of the Regulations, the Economic Court of Alexandria issued a landmark judgment ordering the defendant to pay EGP 10 million in compensation for the unlawful compromise of a customer's personal data. Although the case was brought against a telecommunications operator, it has significant implications for data protection laws.

The Court held that a company may incur civil liability for data protection violations, even in the absence of the Regulations at the time. Liability was established by the Court under general tort law, in particular the custodian's liability concept, and compensation was awarded without any statutory cap, as civil indemnification is not subject to the limits applicable to criminal fines.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

The Centre is currently focused on rolling out the regulatory procedures for filing applications, registrations, and requests for permits and licences, to allow businesses to submit their applications before the end of the grace period, in order to avoid any potential sanctions.

Its practical approach over time will provide greater clarity as to its key priorities. At a general level, however, its direction appears to favour the embedding of a privacy-by-design approach across data processing activities.

Dr. Ibrahim Shehata, Managing Partner at Shehata & Partners Law Firm, has accumulated more than a decade of experience within the Egyptian market. He started his career with Ibrachy & Dermarkar and then Sharkawy & Sarhan law firms before earning his Master of Laws degree in International Arbitration and Venture Capital from New York University. He focuses on corporate law, where he has successfully advised several multinational companies on doing business in Egypt. In the last few years, Ibrahim has been one of the key players in the entrepreneurial ecosystem, helping both startups and venture capital firms navigate legal issues and become more investment-ready.

Shehata & Partners Law Firm
Unit 204, Cairo Business Plaza
New Cairo, Cairo Governorate
Egypt

Tel: +20 102 225 6100
Email: is@shehatalaw.com
LinkedIn: www.linkedin.com/in/ibrahim-shehata-8698258b

Hesham Kamel is a Partner based in Paris, France, with more than seven years of experience in corporate governance, projects, manufacturing, privacy, personal data and cybersecurity. He has a strong academic background, as he holds two Master's degrees from the Sorbonne Law School, both specialising in the international rules governing business and trade. He started his career at Sharkawy & Sarhan, and afterwards joined Shehata & Partners, where he progressed rapidly and became a Partner. Hesham has closed several investment rounds with multiple start-ups and has also been an integral part of multi-million-dollar investment projects.

Shehata & Partners Law Firm
Unit 204, Cairo Business Plaza
New Cairo, Cairo Governorate
Egypt

Tel: +33 768 151 815
Email: hk@shehatalaw.com
LinkedIn: www.linkedin.com/in/hkamel44

Mohamed Abed is an Associate at Shehata & Partners Law Firm. He graduated with honours from Tanta University's Faculty of Law (English Department), ranking fourth in his class. He also holds a Master's degree in Public Law. Prior to joining Shehata & Partners, Mohamed gained valuable experience through internships at prestigious law firms and in-house legal departments, exposing him to various legal areas such as corporate law, contract negotiation, labour law and regulatory compliance. At Shehata & Partners, he specialises in corporate law, labour law and contract drafting, assisting clients with legal documentation, regulatory compliance and employment matters.

Shehata & Partners Law Firm
Unit 204, Cairo Business Plaza
New Cairo, Cairo Governorate
Egypt

Tel: +20 101 493 3315
Email: ma@shehatalaw.com
LinkedIn: www.linkedin.com/in/mohamed-abed-8082671b9

Safa Rabea is an Associate at Shehata & Partners Law Firm, where she advises on a broad range of corporate and regulatory matters, including corporate governance, regulatory compliance and employment law. Her experience spans multiple sectors including assisting with the structuring and implementation of employee equity incentive schemes, as well as providing legal support on transactions and regulatory matters in the pharmaceutical sector. Safa has also been involved in significant industrial projects, advising clients on applicable regulatory frameworks, compliance strategies and project implementation requirements. Her practice is characterised by a strong analytical foundation and a strategic, solutions-oriented approach.

Shehata & Partners Law Firm
Unit 204, Cairo Business Plaza
New Cairo, Cairo Governorate
Egypt

Tel: +20 114 045 4669
Email: sr@shehatalaw.com
LinkedIn: www.linkedin.com/in/safa-rabea

Shehata & Partners Law Firm was founded in 1996 and has been driven by a vision to provide unique legal services that cater to the business needs of corporate entities doing business in Egypt. Its core mission is to provide the most trusted and effective legal advice on both dispute resolution and corporate law in Egypt. The firm is results-driven and delivers exceptional services to clients across various practice areas and multiple industries. It continues to achieve the highest client satisfaction rates in the region due to the meticulous implementation of its client-centric approach.

www.shehatalaw.com

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Data Protection 2026 features three expert analysis chapters and 23 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group