Legal 500
Country Comparative Guides 2026

Egypt
Data Protection & Cybersecurity

Contributor

Shehata & Partners
Law Firm

Ibrahim Shehata

Partner | is@shehatalaw.com

Hesham Kamel

Partner | hk@shehatalaw.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Egypt.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Egypt: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Data protection and privacy are mainly governed by the Personal Data Protection Law No. 151 of 2020 ('**PDPL**') and its executive regulations issued by the Minister of Telecommunication and Information Technology Decree No. 816 of 2025 ('**Regulations**'). These are the main pieces of legislation that govern the collection, processing, storage and cross-border transfer of personal data.

The Personal Data Protection Center ('**Center**') is the authority in charge of enforcing the PDPL. It is responsible for developing and implementing national policies and strategies to protect personal data, as well as setting the standards, procedures, and regulations related to data protection and overseeing their enforcement. It is also mandated with coordinating with public and private entities to make sure that proper data protection measures are in place. Furthermore, it issues the required permits, licences and accreditations.

The PDPL covers personal data electronically processed in full or in part. Consequently, personal data that is fully processed by non-electronic means is not subject to the PDPL.

Some sectors are excluded from the scope of application of the PDPL:

- Personal data retained by individuals and processed for personal use
- Personal data that is processed in order to obtain official statistical data or to enforce a law
- Personal data that is processed for media purposes
- Personal data contained in records of judicial enforcement actions, investigations, and judicial proceedings
- Personal data retained or claimed by the Presidency of the Republic, the Ministry of Defence, the Ministry of Interior, the General Intelligence Service, and the Administrative Control Authority
- Personal data retained by the Central Bank of Egypt and the entities falling under its control, except for money transfer companies and exchange companies

Cybersecurity, on the other hand, is governed by the Cybercrimes Law No. 175 of 2018 ('**Cybercrimes Law**'), which constitutes a complementary legislative source of the PDPL, as it establishes direct criminal protection for personal data and the right to privacy. Unlike the PDPL, the Cybercrimes Law is enforced by the Public Prosecution and the National Telecommunications Regulatory Authority ('**NTRA**').

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

The grace period to comply with the provisions of the PDPL shall end on 31 October 2026. Afterwards, the PDPL shall be in full effect, meaning that the organisations that do not hold a valid licence or permit may be subject to sanctions. Beyond this, there are no expected changes in the data protection, privacy or cybersecurity landscape in 2025 – 2026.

3. Are there any identifiable trends or regulatory priorities in privacy, data protection and/or cybersecurity-related enforcement activity in your jurisdiction?

The issuance of the Regulations in November 2025 triggered a one-year grace period, ending on 31 October 2026. Accordingly, all the addressees of the PDPL are now required to comply with its provisions by applying for the adequate permits and/or licences, adopting the necessary policies and procedures, appointing a data protection officer (DPO) and a local representative for foreign businesses who do not have an presence in Egypt, among other compliance requirements.

Failing to comply by the end of the grace period might

 © 2026 Legalease Ltd

lead to significant penalties, as the PDPL contains an extensive arsenal of administrative and criminal sanctions, including imprisonment and fines.

4. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

The PDPL requires all controllers and processors, regardless of their size, activity, or data volume, to obtain a general licence or permit to undertake their activities as a controller, processor or both. The class of the licence/permit differs primarily as per the volume of data handled by the controller/processor. No exemptions apply at the moment.

Once the general licence/permit is obtained, the data user may need to apply for other special licences/permits, which cover electronic direct marketing, video surveillance systems (e.g. CCTV), and cross-border data transfer.

Failing to obtain a permit or a licence may lead to significant fines, ranging from EGP 500 thousand to EGP 5 million.

In this regard, it is important to explain the difference between a licence and a permit:

- **Licence:** an official document issued by the Center to a legal entity authorising them to process personal data for a renewable three-year period.
- **Permit:** an official document issued by the Center to an individual or a legal entity, authorising them to process personal data for a period not exceeding one year, subject to renewal.

On the other hand, the Cybercrimes Law does not include any registration or licensing requirements.

5. What does “personal data,” “personal information" or other equivalent terms (hereafter “personal data”) mean under data protection laws in your jurisdiction? Does the definition broadly include information about all individuals? For example, would this include individuals acting in a personal or household capacity, as well as those acting in a business or commercial capacity (such as on behalf of a business or corporate entity or employer) or otherwise?

The PDPL defines ‘personal data' as any data relating to an identified or identifiable natural person, whether directly or indirectly, through linking such data with other information such as name, voice, image, identification number, online identifier, or any data that reveals psychological, health, economic, cultural, or social identity.

This definition is broad enough to include all sorts of information that may lead to identifying an individual, regardless of whether this individual acts in a personal or household capacity, as well as those acting in a business or commercial capacity.

Moreover, the elements mentioned in the legal definition above are referred to by way of illustration, and not as an exhaustive list. This means that other types of data that are not necessarily mentioned in the definition (e.g., geolocation data, sexual orientation, hobbies) may also serve as ‘personal data' if they lead to identifying an individual through linking such data with other information about them.

6. Are certain types of personal data considered more sensitive or highly regulated under data protection laws in your jurisdiction? Please include the relevant defined terms for such data (e.g., special categories of personal data," “sensitive data” or “sensitive personal information"?

The PDPL provides a special definition for ‘sensitive personal data', which means data that reveals mental, psychological, physical, or genetic health, biometric data, financial data, religious beliefs, political opinions, or security status. And in all cases, children's data shall be deemed sensitive personal data.

By way of comparison, the PDPL classifies certain types of data as sensitive that are not treated as such under the GDPR. This includes financial data, security status, and children's data (while not sensitive by default, children's data still benefits from specific protection under the GDPR).

7. What principles apply to the processing of

 © 2026 Legalease Ltd

personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

In its guidelines, the Center fleshed out nine principles that apply to the collection of and processing of personal data, based on the PDPL and the Regulation:

- **Lawfulness:** 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, defending a legal claim or right, and execution of court judgments or orders issued by competent investigative authorities.
- **Fairness:** personal data should be processed in a manner that aligns with data subjects' reasonable expectations, and ensure that data subjects 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, as per Article 3 of the PDPL.
- **Transparency:** personal data must be processed in a manner that is transparent, clear and honest towards the data subject. This also may result from Article 3 of the PDPL, which requires the data user to declare the processing purposes to the data subject.
- **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 is an obligation upon the controller, to verify the adequacy of data collected (Article 5, PDPL).
- **Data accuracy:** personal data must be accurate, complete and kept up-to-date, in line with the purposes of the processing activity (Article 3, PDPL).
- **Storage limitation:** personal data must not be retained for longer than necessary to achieve the purposes of the processing activity (Article 3, PDPL).
- **Data security:** personal data must be secured throughout its entire lifecycle against unlawful or unauthorised processing, access, alteration, damage, loss or destruction (Article 3, PDPL).
- **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 (Articles 4 and 5, PDPL).

These principles reflect the Center's intention to implement a privacy by design framework, ensuring that personal data is protected and that the rights of data subjects are safeguarded from the outset.

8. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Consent is one of the legal bases upon which a data user may collect and process personal data. As one of the most used bases, the PDPL, the Center indicates in its guidelines that a consent must be provided directly by the data subject, in an explicit and clear manner, and the data subject must have been informed about the purposes for which their data is collected/processed.

Furthermore, consent must be granular and given for specific, separate purposes, and not bundled with other matters.

Another important aspect of the consent is how appropriate it is as a lawful basis. For instance, the Center emphasises that consent must be freely given. Therefore, in situations where there is a power imbalance (e.g., employment relationship), or where personal data is being processed regardless of consent (e.g. entering a mall where there is CCTV and asking for consent), consent may not be the most appropriate basis.

 © 2026 Legalease Ltd

Additionally, the Regulations stipulate that consent can be implied. This is where the data subject is freely giving their personal data in exchange for products or services, provided that the given consent remains limited to its initial purpose, and not unlawfully extended afterwards.

In all cases, a data subject must retain the right to revoke their consent at any time maintained.

9. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

As a pre-condition, a data user must be a holder of the general licence or permit that allows them to process personal data. Moreover, to collect and process sensitive personal data in particular, a data user must obtain the explicit and written consent of the data subject, whether in paper form or through electronic means.

In addition to consent, the collected data must be essential and necessary for the special purpose of their processing, and may not lead to causing harm to the data subject.

The Center might issue further guidance on this matter.

10. Do the data protection laws in your jurisdiction have special or particular requirements, restriction, or rules regarding the collection, use, disclosure or processing of personal information from or about children or minors? If so, what is the age threshold and key requirements/restrictions that go beyond those applicable, generally?

The PDPL makes additional requirements in case of processing children's data, as follows:

- If the child is under 15 years old, a valid consent must be obtained from the child's guardian in writing and in an explicit manner. Further, it must be limited in time, and may be revoked later on.
- If the child is at least 15 years old, the child, or their guardian, must give their written consent.
- In case of having the child participate in a game or a competition, the requested data must be limited to what is strictly necessary. Moreover, such data may not be later used in any operations involving profiling, tracking or behavioural monitoring of children.

11. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Beyond the sectors excluded from the scope of the PDPL, as explained in the first question of this guide, the PDPL does not provide for any derogations, exemptions, exclusions, or limitations to its obligations. Accordingly, requirements such as obtaining a permit or licence and appointing a DPO and a representative in Egypt apply to all data users, regardless of their size or type of business.

12. Does your jurisdiction require or recommend privacy risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

In its guidelines, the Center requires data users to conduct the necessary data protection risk assessments, including legitimate interest assessment and transfer impact assessments. Such assessments must be properly documented and made available to the Center upon request.

13. Are there any specific codes of practice, or self-regulatory codes applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

At present, no specific codes of practice or self-regulatory codes have been formally adopted.

14. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

All organisations, whether acting as controllers or processors, are required to maintain a RoPA and implement internal processes documented in writing. The

 © 2026 Legalease Ltd

nature and content of these obligations vary according to the capacity in which the organisation acts.

For the RoPA, the minimum information required from all data users includes:

- Consent of the data subject, its issuance date and form
- Description of the categories of personal data collected and processed
- Retention periods of each category of personal data
- Organisational and technical procedures implemented to secure the data, in a manner that enables the Center to conduct its periodic control

Internal processes and documentation should cover key aspects of data governance and protection, including:

- Data management and classification policies, governing the collection, storage, identification, and retention of personal data, including sensitive data and anonymisation practices where applicable.
- Data quality and integrity controls, including periodic testing and evaluation processes to ensure the accuracy and reliability of the data held.
- Technical and organisational security measures (TOMs), aimed at ensuring the confidentiality, integrity, and resilience of processing systems, including the ability to restore availability and access to personal data in the event of physical or technical incidents, and compliance with the security standards set by the Center for handling sensitive personal data, including children's data.
- Data subject rights procedures, providing mechanisms that allow individuals to access their personal data, withdraw consent, request rectification, restrict processing to a specific scope, and object to processing, in accordance with mechanisms approved by the Center.

15. Do the data protection laws in your jurisdiction specifically impose data retention limitations? If so, please describe such requirement(s).

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.

16. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

There is no mandatory requirement under the PDPL for such consultation.

17. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

All data users are required to appoint a data protection officer. The legal responsibilities of a DPO include:

- Performing a regular evaluation and inspection of the personal data protection systems
- Acting as a point of contact vis-à-vis the Center, and implementing its decisions
- Enabling data subjects to exercise their rights
- Notifying the Center of data breaches and infringements
- Monitoring the implementation of the security policies issued by the Center in relation to securing the processing, storage and handling of data
- Submitting an annual report to the Center on the state of privacy protection at the data user, or upon request
- Monitoring the process of receiving reports and complaints of data subjects with respect to deleting, modifying or supplementing their personal data, and ensuring their execution

18. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

A DPO is mandated to organise training programmes for the employees of the data user they serve. Failure to comply with this obligation may result in a fine. The PDPL does not provide any details on this requirement.

 © 2026 Legalease Ltd

19. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

The PDPL requires controllers to provide notice to data subjects of their processing activities. In its guidelines on privacy notices, the Center requires that a written notice include a minimum amount of information, such as the identity of the controller, DPO's contact details, categories of personal data collected, lawful basis of processing, purposes of processing, retention period, among other things.

Further, the Center requires that the notice is written in Arabic (other languages may be added), intelligible, transparent, concise, visible and easily accessible.

A privacy notice may be either written, for example on a website, or verbal, for example during phone calls or in-person collection.

20. Do the data protection laws in your jurisdiction distinguish between the responsibilities of "controllers" and those of "processors" (or equivalent terms) of personal data? If so, how are such terms defined and what are the key distinctions between the obligations of controllers and processors (or equivalent terms)?

The PDPL distinguishes between them as follows:

- 'Controller' means any natural or legal person who, by virtue or nature of their work, has the right to obtain personal data and determine the method, manner, and standards for retaining, processing, or controlling such data in accordance with the specified purpose or their activity.
- 'Processor' means any natural or legal person who, by virtue of the nature of their work, processes personal data for themselves or on behalf of the controller pursuant to an agreement with the controller and in accordance with its instructions.

While controllers and processors share similar responsibilities (for example, obtaining a licence or a permit, implementing technical and organisational security measures, appointing a representative in Egypt, maintaining RoPAs), a controller has the decision-making power to decide how personal data would be processed. Therefore, controllers have broader responsibilities related to the lawfulness and governance of data processing, as well as the integrity and accuracy of the data collected.

Processors, by contrast, are primarily responsible for the execution of processing operations within the limits defined by the controller and the PDPL.

21. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

As a general rule, automated decision-making and profiling need to be carried out on a lawful basis, while following the main data processing principles, such as data minimisation, transparency, and proportionality. Furthermore, a data subject may not be harmed, and their fundamental rights and liberties must be upheld.

Use of cookies and tracking technologies for electronic direct marketing (EDM) purposes is subject to EDM obligations, including obtaining the data subject's prior valid consent.

As for children's data, it is prohibited to use their 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.

22. Do the laws in your jurisdiction include specific rules, requirement or regulator guidance regarding the use of cookies, pixels, online tracking and/or targeted advertising? Please describe any restrictions on targeted advertising and/or cross context behavioral advertising. How are these terms or any similar terms defined?

Under the general principles of the PDPL, the use of online tracking technologies, including cookies, software development kits (SDKs), and other device identifiers, requires obtaining the prior, explicit, and valid consent of the data subject. Where such technologies are used for marketing purposes, they are additionally subject to the rules on electronic direct marketing.

Consent must be obtained through fair and transparent

 © 2026 Legalease Ltd

means. Misleading consent practices, including dark patterns or interfaces designed to influence user choices, invalidate consent, as it cannot be considered freely given, explicit, or informed.

Each electronic marketing communication must include a clear and effective 'unsubscribe' mechanism. Where such a mechanism exists only in form but is ineffective in practice, or where marketing communications are disguised as personal messages, the processing is unlawful.

23. Do the data protection laws in your jurisdiction specifically restrict or regulate the "sale" of personal data and/or "data brokers"? How is "sale" and/or "data broker" or (similar/related terms) defined?

Egyptian law does not specifically regulate the sale of personal data or data brokers. However, as this operation qualifies as an act of processing, it is recommended to abide by the PDPL general rules and principles, especially those related to processing data on a lawful basis.

In case the sale of data would lead to transferring the data abroad, a licence or a permit would be required from the Center.

24. Do the data protection laws in your jurisdiction specifically regulate or restrict marketing and electronic communications, including telemarketing/telephone solicitations and 'robocalls', email marketing, SMS/text messaging or other direct marketing? Please provide an overview.

These operations all qualify as electronic direct marketing. Therefore, they are subject to the same obligations presented under question 22.

25. Do the data protection laws in your jurisdiction regulate, restrict or impose specific obligations on the processing of biometric data, such as facial recognition. If so, how are the relevant terms defined? Are these obligations focused on the collection, use and processing of unique biometric 'identifiers' (rather than any sort of biometric measurements) ?

Biometric data is classified as sensitive personal data under the PDPL. Therefore, they are subject to the same obligations presented under question 9. Further guidance may be issued by the Center with respect to certain technologies such as facial recognition.

26. Are there any data protection laws in your jurisdiction that specifically address or apply to artificial intelligence or machine learning ("AI"). If so, do these laws specifically apply to the processing of personal information related to AI, or more broadly?

Egypt does not currently have a standalone law regulating AI. Accordingly, the use of personal data in the training, development, or operation of AI systems or models is governed by the PDPL and its Regulations.

Any processing of personal data in this context must comply with the general data protection principles set out under the PDPL, including lawfulness, purpose limitation, data minimisation, data accuracy, storage limitation, integrity and confidentiality, and accountability.

Under the Regulations, where personal data is used to train or operate AI models, the legal obligation imposed on data processors is limited to compliance with 'locally, regionally, and internationally recognised standards.' This includes the Egyptian Charter for Artificial Intelligence, a soft law document issued by the National Council for Artificial Intelligence. This Charter includes the common international standards, such as human-centeredness, transparency and explainability, fairness, security and safety, and accountability, and covers the AI's use in both public and private sector.

27. Are there any data localization requirements in your jurisdiction? In other words, are there any circumstances where some or all personal data is required to be stored locally, or prohibited from being transferred to or stored in certain jurisdictions?

Any cross-border transfer of personal data is prohibited unless it is carried out in accordance with the conditions expressly set out in the PDPL and its Regulations, and subject to obtaining the required licence or permit from the Center.

Additionally, the Supreme Council of Digital Society published a governmental cloud-first policy which includes some requirements on data localisation. It recommends that the localisation of data classified as

 © 2026 Legalease Ltd

'top secret' or 'secret,' requiring that such data be hosted exclusively within Egypt. This applies to data related to national security or sensitive operations and aims to ensure maximum protection against unauthorised access, breaches, or manipulation.

28. Is the transfer of personal data outside your jurisdiction restricted, under certain circumstances? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Cross-border transfers of personal data in Egypt are regulated under the PDPL and its Regulations. However, 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.

With respect to the mechanisms and assessments required for cross-border lawful transfers, the PDPL and its Regulations set out the key requirements applicable to any data controller or processor as follows:

- As general rule, the PDPL and its Regulations prohibit the transfer, storage or sharing of personal data outside Egypt unless the destination country ensures a level of data protection not less than the level prescribed under the PDPL and its Regulations.
- 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, specified under Article 15 of the PDPL.
- The controller or processor must obtain a licence or a permit from the Center, based on its assessment of the adequacy of the level of protection in the destination country.
- The controller or processor must obtain the consent of the data subject for the cross-border transfer.
- 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.
- 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, and therefore the approval of the Center.

Moreover, onward transfers are permitted only where the activities of the relevant controllers or processors are compatible or integrated, or serve a legitimate interest of the parties or the data subject, and provided that the level of legal and technical protection applied by the controller or processor located abroad is not less than the level applicable in Egypt.

29. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

The PDPL and the Regulations present the security obligations in broad terms, and require that personal data be secured throughout its entire lifecycle. This is to maintain the integrity, confidentiality, availability of both the personal data and the processing systems, as well as to maintain the resilience of such systems. Both controllers and processors are addressed with such obligations.

If processing activities present a high risk to the rights and freedoms of data subjects, proportionate and where necessary, enhanced security measures must be implemented.

These obligations should be detailed by the Center in its future guidelines and practice, especially when approving permits and licences.

30. Are there more specific security obligations for certain types of personal data (e.g., sensitive data or special categories of personal data)?

The Center may issue more specific security obligations for sensitive personal data.

31. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances and within what timeframe must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

 © 2026 Legalease Ltd

A 'personal data breach and infringement' is defined under the PDPL as any unauthorised or illegal access to personal data, or any other illegitimate operation to reproduce, send, distribute, exchange, transfer, or circulate which aims to expose or disclose such personal data, or damage or edit the same while being stored, transferred or processed.

In such case, the Center must be notified 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. Notification 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.

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

The Center may investigate breaches, request information and co-ordinate with national security authorities where applicable. Non-compliance may result in administrative or criminal sanctions.

32. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

Under Article 2 of the PDPL, personal data may not be collected, processed, disclosed or made available by any means except with the explicit consent of the data subject or in cases expressly permitted by law. In this context, the data subject is granted the following rights:

- To be informed of, access, review and obtain personal data held by any data holder, controller or processor
- To withdraw consent previously given for the retention or processing of personal data
- To request the correction, amendment, updating, addition or deletion of personal data
- To limit the processing of personal data to a specific scope
- To be informed of any breach or violation affecting personal data
- To object to the processing of personal data or its outcomes where such processing conflicts with the data subject's fundamental rights and freedoms

Except for the right to be informed of data breaches, the exercise of these rights may be subject to a service fee payable by the data subject to the controller or processor, as determined by the Center and within the legally prescribed limit.

The practice of the Center in the future might lead to specifying further rights for data subjects, based on its interpretation and the implementation method of the law.

33. Do the data protection laws in your jurisdiction allow or provide for a private right of action for violations? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action applies and/or a class action may be brought, and whether types of claims/violations present a higher risk of a private right of action or class action (e.g., are there statutory damages or presumed harm for certain violations)?

There is no general legislative framework allowing a claim to be brought on behalf of an undefined group of affected persons, including in privacy or data protection matters.

Alternatively, the civil and commercial procedures law allows multiple claimants to 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. This mechanism does not constitute collective redress in the technical sense.

Furthermore, in data protection matters, data subjects may file complaints with the Center. The Center's decisions are administrative in nature and do not amount to judicial collective redress or collective compensation.

34. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Individuals are entitled to monetary compensation if they

 © 2026 Legalease Ltd

are affected by breaches of the PDPL. The assessment and quantification are subject to the general principles of tort law, and may include actual and material damage as well as non-material damage. This has been showcased in a recent judgment issued by the Alexandria Economic Court in September 2025, ordering the defendant to pay EGP10 million in compensation for the unlawful compromise of a customer's personal data.

35. How are data protection laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

The Personal Data Protection Center is the primary authority responsible for enforcing the PDPL. It is mandated with regulating activities related to personal data processing, issuing the required permits and licences, making national policies and guidelines, investigating violations and receiving complaints.

Nonetheless, as it was only established recently, and there is currently a grace period extending until 31 October 2026, the Center is not yet fully utilising its regulatory powers.

36. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

The PDPL also includes two sets of sanctions: administrative and criminal.

For administrative sanctions, the Center shall first deliver a warning to the concerned person who is found to be in violation of the PDPL, and shall require them to comply within a specified duration. Following the lapse of this duration without having complied with the PDPL, the Center may deliver another warning, suspend or revoke the licence/permit, and subject the concerned person to its scrutiny.

For criminal sanctions, the PDPL includes an extensive arsenal consisting of fines and imprisonment penalties. Sanctions are primarily intended to penalise breaches of personal data confidentiality, prevent data subjects from exercising their aforementioned rights, and any general violations of the obligations of the controller or processor as outlined by the PDPL.

Thus, violating the provisions related to permits, licences or accreditations may result in the imposition of a fine ranging from EGP 500 thousand to EGP 5 million.

Currently, there are no publicly accessible guidelines or rules for the calculation of such fines or the imposition of sanctions

37. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, as the Center's decisions are of an administrative nature, the concerned party may appeal before the administrative courts.

38. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide an overview of these obligations and explain their scope/applicability. For example, are all organizations subject to the requirement or only to certain organizations (e.g., based on size, sector, critical infrastructure designation, public company)? Are there specific and/or additional regulations for different industries (e.g., finance, healthcare, government)?.

The Cybercrimes Law requires service providers to implement specific cybersecurity risk management measures and undertake defined actions in this regard, failing which they may be subject to a fine or imprisonment.

A 'service provider' is legally defined as any individual or legal entity who provides users, whether they were individuals or legal entities, with information and communication technology services. This includes any person who processes or stores information, whether directly or on behalf of others, in relation to any of those services or information technology.

Under the Cybercrimes Law, a service provider is required to:

- Retain and store system and user-related data for 180 consecutive days
- Keep data that enables identification of users, as well as data on content, communications traffic, and devices used
- Preserve the integrity of stored data and

 © 2026 Legalease Ltd

prevent any unauthorised alteration or disclosure
- Refrain from disclosing data except pursuant to a reasoned order from a competent judicial authority
- Ensure the confidentiality and security of data against breaches, loss, or damage
- Provide users and competent authorities with clear, accessible identification and contact information
- Disclose licensing details and the relevant supervisory authority
- Provide any additional information required by regulators for user protection
- Provide technical capabilities to national security authorities upon request, in accordance with the law
- Collect user data in the course of providing or marketing services, and ensure that no unauthorised parties do so

The executive regulations of the Cybercrimes Law, issued by virtue of Prime Minister Decree No. 1699 of 2020, add further technical details on the specific implementation of the above obligations.

39. Do the cybersecurity laws in your jurisdiction impose formal cybersecurity audit or certification requirements? If so, please provide an overview.

The Cybercrimes Law does not impose such a requirement. However, if a company wants to provide cybersecurity as a service, it needs to get a licence from the NTRA.

40. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding vendor and supply chain management? If so, please provide details of these requirements.

The Cybercrimes Law requires that the collection of users' data to be done only by service providers, along with their authorised commercial chain (agents and distributors). No other unauthorised parties are permitted to do so.

41. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, please provide an overview of the requirement, including whether there are any formalities that must be observed regarding such appointment (e.g., board-approval, reporting line structure, notification to regulatory body).

Service providers are generally required to provide contact information to users and competent governmental authorities.

If the service provider owns, manages, or operates a critical information infrastructure, they must clearly define the responsibilities of senior management and personnel responsible for information technology and cybersecurity. These responsibilities should be aligned with the organisational structures, job roles, and training programmes established by the human resources function.

A 'critical information infrastructure' is legally defined as a set of essential information systems, networks, or assets, the disclosure of whose details, or their disruption, or the alteration of their operation in an unlawful manner, or unauthorised access thereto, or unlawful access to the data and information they store or process, or the commission of any other unlawful act affecting them, would result in impacting the availability of essential State services and facilities, or causing significant economic or social losses at the national level.

42. Do the cybersecurity laws in your jurisdiction impose specific reporting or notice obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and what are the reporting and notification requirements (please also note whether these laws require reporting of certain cyber security incidents, regardless of whether there has been a 'breach of personal data')?

If the service provider owns, manages, or operates a critical information infrastructure, it must notify the Egyptian Computer Emergency Readiness Team (EG-CERT) of any unauthorised access incidents or breaches as soon as possible.

These incidents and breaches fall under the legally defined term 'hacking', which means an unauthorised access, or violation of licensing terms, or accessing by any unlawful means an information system, computer, or information network, or any equivalent thereof.

 © 2026 Legalease Ltd

43. Can individuals bring a private right of action for cybersecurity incidents or other violations of cybersecurity laws? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action and/or a class action may be brought?

Individuals may bring a private right of actions for cybersecurity incidents or other violations as indicated under the Cybercrimes Law, subject to the civil and criminal procedures laws.

Regarding 'class action' litigation, please refer to our answer to question 33.

44. How are cybersecurity laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

While the NTRA plays a significant role in enforcing the Cybercrimes Law, it works in conjunction with the judicial and investigation authorities who take a leading role, primarily the Public Prosecution. This is due to the criminal nature of the Cybercrimes Law.

45. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Judicial and investigation authorities are competent to enforce the Cybercrimes Law as follows:

- Issuing reasoned orders to seize, collect, preserve, or track data, information systems, and electronic devices
- Conducting searches and accessing computer systems, programmes, databases, and other information technologies
- Compelling service providers to disclose stored data, user data, and communication traffic data under their control
- Ordering the blocking of websites or online content that constitute offences or threaten national security or the economy
- Implementing urgent temporary blocking measures through coordination with competent authorities and service providers, and referring blocking orders to the competent court for review and approval within legally prescribed timeframes
- Imposing travel bans on suspects and placing them on watchlists where necessary and supported by sufficient evidence

46. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction? What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

The Cybercrimes Law has an extensive sanctions framework. It applies to offences against the integrity of information networks and systems, the unlawful use of telecommunications and information technology services, crimes committed through information technologies, fraud and offences involving bank cards and electronic payment tools, as well as violations of privacy and the dissemination of unlawful digital content. Sanctions range from fines to imprisonment, depending on the nature and severity of the offence.

Currently, there are no publicly accessible guidelines or rules for the calculation of such fines or the imposition of sanctions

47. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, this would be through the existing legal and judicial frameworks.

Contributors

 © 2026 Legalease Ltd

Ibrahim Shehata
Partner
is@shehatalaw.com

Hesham Kamel
Partner
hk@shehatalaw.com

 © 2026 Legalease Ltd