COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Egypt

DATA PROTECTION & CYBERSECURITY

Contributor

Mena Associates in association with Amereller Rechtsanwälte

Dr. Ingy Rasekh

Managing Partner (Cairo) | rasekh@amereller.com

Nisreen Al-Karyouti

Partner (Cairo) | karyouti@amereller.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 by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

General Protection

a. The **Egyptian Constitution** includes general principles which imply that laws should protect individual's right to privacy, the inviolability of citizens' private life , as well as the protection of correspondence, telephone calls and any other means of communications which may only be confiscated, examined or monitored by virtue of a judicial order for a limited period in the circumstances stipulated by law (Article 57).
b. The **Egyptian Telecommunication Regulation Law**, which provides for the privacy of telecommunications and imposes penalties for infringement of its regulations.
c. The **Egyptian Civil Code**, which grants general protection, under tortious liability, against the infringement of private data, if the data subject suffers damages.
d. The **Penal Code**, which provides sanctions for disclosing, facilitating the disclosure of, or using a recording or document obtained by recording or transmitting via private conversations or telephone by any method; shooting, taking, or transmitting a picture of anyone in a private place by any means, without the consent of the photographed party. (Article 309 bis) Article 309 bis (A) further penalizes the broadcasting of any recording or document in the manner prescribed under Article 309 bis. Private places are defined by the Court of Appeal as "*Any place in which a person resides permanently or temporarily*". [CA 674 of 56 J – hearing of 4/6/1986]
e. The **Labour Law**, which protects employee personal data (such as name, job, professional skills, workplace, domicile, marital status, salary, employment starting date, holiday leave, workplace sanctions, and employee reports) and states that employers must keep employee personal data for at least one year from the end-date of the employment relationship.
f. The **Banking Law**, which stipulates that all bank customer accounts, deposits, trusts, safes, and their related dealings must remain confidential, except with the written permission of the owner of the account, deposit, trust, or safe; the account owner's successors, anyone to whom all or some of such funds have been bequeathed; or a legal representative or authorized attorney or pursuant to a judicial ruling or an arbitral award. (Article 97).
g. The **Competition Law**, which imposes confidentiality obligations on its officials and employees, relating to all information related to individuals and corporations (Article 16).

Personal Data Protection Law No. 151 of 2020 ("PDPL")

Personal Scope (Article 1) – Any holder, controller, or processor in relation to natural persons shall be protected under the regulation.

Territorial Scope (Article 2) – The Data Protection Law is applicable in case of breach, which results consequently to any of the following:

- An Egyptian national on national grounds or abroad
- A non-Egyptian residing in Egypt
- A non-Egyptian residing outside Egypt if the act is punishable in said country and the data subject affected by the breach is an Egyptian

national or non-Egyptian residing in Egypt.

Material Scope (Article 1) – It applies to any personal data that is partially or entirely subject to electronic processing. Article 3 provides the personal data that is not applicable under the Law:

- Saved by natural persons for third parties and that is processed only for personal use.
- Processed in relation to the application of laws and/or regulations in Egypt or is processed for official statistics purposes.
- Processed specifically for media purposes, if the personal data is correct and is not used for any other purposes without prejudice to any applicable media regulations.
- Related to judicial seizure warrants, investigations or lawsuits.
- Held by national security.
- Held by the Central Bank of Egypt and the entities subject to its control and supervision. An exception applies in the case of money transfer and foreign exchange companies, if they consider the rules established by the Central Bank that regulate personal data.

Exclusions– The Promulgation Articles of the PDPL expressly exclude from the scope of the law, *inter alia*, the personal data collected and/or processed by the national security authorities. We understand this exclusion from the protection provided in the PDPL to allow said authorities to access and process personal data whether for the use inside or outside the country if such collection is related to the work of such authorities. The National Security Authorities are defined as the Presidency, Ministry of Defense, Ministry of Interior, General Intelligence Service, the Administrative Control Authority.

General Principles of PDPL:

- Collection, storing, processing and transferring of personal data, entails prior permission of the data subject, save as otherwise expressly provided under the Law.
- The data subject has the right to know what data are being collected, stored, processed and/or transferred. They further have the right to set restrictions on the said, and to amend the data. In any case, they have the right to revoke their consent. They have the right to know in case of any violation and may oppose to any processing or the result thereof if it does not conform with their rights.
- The collection of data entails that such collection is for legitimate purposes, that the information is accurate. The processing of the data must be in legitimate means and within the limits of the purpose of their collection. The storage of collected data shall not be for longer than the period necessary for its collection. The Executive Regulations shall set forth the relevant regulations and thresholds.
- In the event of a data breach e.g. by a third party, the controller is obliged to report said breach within a maximum of 72 hours. Direct marketing using personal data is prohibited, except if certain conditions are satisfied including, inter alia, the data subject's consent.
- The Law requires consent for direct electronic marketing and requires that the data subjects are provided with an easy mechanism to not grant their consent, opt out and/or revoke it. It further requires that the sender's identification and address are clearly specified in a manner facilitating for the data subject to reach out to them, and that the correspondence clearly indicates that it is for marketing purposes. The advertiser must maintain records of the data subject's consent for three years from sending the last related correspondence.

Enforcement of the Law (Article 19) – The Data Protection Centre (DPC) is responsible for overseeing the enforcement of the Data Protection Law. This entails the issuance of any necessary licenses as well as the authorization and certification in line with the Data Protection Law. (The DPC however is not yet operational).

The Cabinet has yet to issue the Executive Regulations of the Personal Data Protection Law. This will further clarify the law's provisions and how it is to be enforced.

Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 (Executive regulation No. 1699 of 2020) ("Cyber Crimes Law")

The service providers are under a duty to:

- maintain the privacy of data stored with them and shall not disclose said data without a judicial order. This includes, inter alia, data enabling the identification of the service user, or any data or information related to the sites and private accounts accessed by said users.
- secure the data and information in a manner maintaining their confidentiality and protecting them against hacking and damage.
- provide the service users with certain data and information in an easy and accessible manner. Said information includes name and

address of the service provider, contact information such as an email address, registration information, and any other information which is deemed important by the Egyptian National Telecom Regulatory Authority (NTRA) for the purpose of protecting the service users.

retain certain data for 180 consecutive days, in accordance with Article 2 of the Law. Such data includes data enabling the identification of the service user, data related to content and the context of the information system in which it is being processed and traffic-related data and communication terminals. The Law prohibits sending spam emails to a certain person without obtaining their consent as well as the provision of personal data to systems or websites for the purpose of promoting goods or services without the consent of the respective person.

Article 25 of the Cyber Crimes Law punishes, inter alia, the violation of the private life and giving out the personal data to any system or website to promote goods or services, or publishing the same via internet or through any information technology means, without the consent of the person to whom such data is related. Such acts are punishable with imprisonment of not less than 6 months and/or a fine ranging between EGP 50,000 and 100,000.

Consumer Protection Law Article 29 of Law No. 181 of 2018

Supplier of products or services shall keep confidential the consumer's information and his private data and may not disclose or transfer the same unless otherwise expressly authorized by the consumer.

The supplier shall further take all the necessary precautions to protect the confidentiality of such information and data.

The definition of supplier under the law extends, inter alia, to manufacturers, exporters and distributors located outside Egypt for goods and services sold in Egypt.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

The Personal Data Protection Act was promulgated by Law No. 151 of 2020 on July 13th, 2020. The Executive Regulations should have been issued and published within six months from the date on which the Law entered into force. The said deadline corresponds to 14 April 2021. However, the Executive Regulations have not been issued to date. To our knowledge, a team of experts has been formed within the Minister of Telecommunications to develop a draft of the Executive Regulations and discuss it with the relevant stakeholders. We are informed that said team has been given a timeline of one year to finalize the draft and present it to the Cabinet for approval so it is currently anticipated that the Executive Regulations will be passed within 12-18 months.

3. Are there any registration or licensing requirements for entities covered by these laws, and, if so, what are the requirements? Are there any exemptions?

In Egypt, there are no data localization requirements. In other words, there are no laws that require "physical" storage of Personal Data or to locally host infrastructure.

However, pursuant to the PDPL, cross-border Personal Data transfer is now subject to certain restrictions.

Article 1 of the Law defines cross-border transfer as *"transferring, making available, recording, storing, circulating, publishing, using, displaying, sending, receiving, retrieving or processing Personal Data from inside the Arab Republic of Egypt overseas or vice versa"*. A prior permit by the 'Personal Data Protection Center' (the Center) is required for the collection, storing, processing and transferring of sensitive personal data, as well as data processing in general (i.e. regardless of the sensitivity of the personal data), and cross-border transfer of data. Further details are yet to be specified under the Law's Executive Regulations upon their enactment.

According to Article 1 of the PDPL, licenses issued by the DPC for controllers or processors are valid for three years and can also be renewed thereafter.

In addition, according to the Cybersecurity Law and its Executive Regulations, which concern any person providing, directly or indirectly, users with any information technology and telecom service, including, *inter alia,* processing or data storage, such providers are required to retain and store users' data continuously for at least 180 days, including identification, content of the services' system, communication traffic, terminals and any other data required by the National Telecommunication Regulatory Authority.

4. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

Personal data is defined as "*all data that is related to a natural person. A person who is already determined or can be determined, either directly or indirectly, through relating data with any other data including name, voice, identification number, and data determining psychology or physical health, economic status, or cultural social identity*".

Sensitive data is defined as "*any data that entails psychological, mental, physical, or genetic health data, biometric data, financial data, religious belief, political opinion, or security conditions and, in all cases, children's data, is considered sensitive personal data".*

Data controller is defined as "*any natural or juridic person who, based on the nature of their work, has the right to obtain personal data and to determine the process and the criteria of keeping or processing personal data and control it based on the determined purpose".*

Data processor is defined as "*any natural or juridic person whose work involves the processing of personal data for their own benefit or the benefit of the data controller, as set forth by an agreement with the data controller and the instructions thereof."*

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Under Articles 3 of the PDPL, the storage and processing of personal data must be carried out in according to the following principles:

- Data Minimization: personal data must be collected for legitimate, specific and transparent purposes known to the data subject.
- Accuracy and Security: personal data must be correct, valid and secure.
- Lawfulness: personal data must be handled in a lawful manner and appropriate for the purposes for which it was collected
- Storage Limitation: personal data should not be held for a longer period than is necessary to fulfill its purpose.

The legal bases for the collection and processing are the following:

- Consent – Article 2 of the Personal Data Protection Law, states that personal data may only be collected, processed, or disclosed if explicit consent of the data subject is given. Article 6 further requires the data subject to provide consent as one of the conditions for the processing of personal data.
- Contract or Legal Obligation – Article 6 states that the processing of personal data shall be legal if it is required for the performance of a contractual obligation, a legal action, the execution of an agreement for the benefit of the data subject, or to undertake necessary procedures to claim or defend the data subject's legal rights. Furthermore, the processing of personal data shall also be legal if it is required to perform an obligation as regulated by the Personal Data Protection Law, based on a court order or an order issued by the regulatory authority.
- Interests of the data subject – According to Article 6, the processing of personal data shall also be allowed if it is necessary for the performance of a contractual obligation, a legal action, the execution of an agreement for the benefit of the data subject or to go through a procedure to claim or defend the data subject's legal rights.
- Legitimate interest of the data controller – Article 6 states that the processing of personal data shall be legal if it is necessary to meet the legitimate rights of the controller or any relevant person unless it goes against the basic rights and freedoms of the data subjects.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

Article 2 of the PDPL stipulates that any personal data may only be collected, processed or disclosed with the explicit consent of the data subject. Article 6 also states that consent by the data subject is one of the conditions for the processing of personal data.

7. 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 must be explicit as stipulated by Article 2 of the PDPL. The Executive Regulation, once issues, is expected to further clarify the form, content and administration of such content.

8. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection or disclosure?

According to Article 12, the controller or processor must be licensed by the DPC to legally collect, transfer, store, keep, process and make available any sensitive personal data.

Unless legally permissible, an explicit written approval shall first be obtained from the person concerned (Article 12).

The criteria for the aforementioned conditions and restrictions are to be identified by the Executive Regulation implementing the PDPL.

9. How do the laws in your jurisdiction address children's personal data?

Under Article 12 of the PDPL, children's data is classified as sensitive data and provides that the transfer, collection, storage, or processing of such data shall not be made except with the consent of the legal guardian.

Any individual under the age of 18 years is considered a child (Article 2 of the Child Law No. 12 of 1996).

10. How do the laws in your jurisdiction address health data?

Health data, although not clearly defined under the PDPL, is considered sensitive data.

11. Do the laws include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

Please see the exclusion of national security authorities from the PDPL explained under our answer to question 1. Further derogations, exclusions or limitations may be identified by the Executive Regulations of the PDPL , which are yet to be issued.

12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

It is unclear whether requirements of 'data protection by design' or 'data protection by default' will be imposed as the Executive Regulation is yet to be issued.

On the other hand, any natural or juridic persons that wish to process personal data are necessarily required to follow the PDPL when it comes to the processor's obligations. Part of abiding by the PDPL, is appointing a Data Protection Officer ("DPO"), a legal representative of a legal person that any data processing or controlling entity must appoint within its internal corporate structure. The role of the Data Protection Officer as stated by Article 8 is to be further clarified by the Executive Regulation, once it is issued.

13. Are owners/controllers or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Article 4 of the PDPL stipulates that controllers of personal data shall keep a special record of data that includes a description of the categories of personal data it retains, specifying who disclosed or made the data available to the controller, its documentation, time period, restrictions, scope, mechanisms for erasing or modifying personal data, and any other data related to transfer or personal data across borders and a description of technical and organizational procedures of data security.

According to Article 5 of the PDPL processors of personal data shall prepare a record of processing operations. These processing operations include the categories of processing, which the processor performs on behalf of any controllers and its contact details and its DPO, processing times, restrictions, scope, mechanisms for erasing and modifying personal data, and a description of the technical and organizational procedures for data security and processing.

14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

According to Article 1 of the Personal Data Protection Law, the DPC license issued for controllers or processors are valid for three years, after which they can be renewed.

Any person providing users, either directly or indirectly, with any information technology and telecom service, including the processing or storage of data, are required to retain users' data continuously for at least 180 days, including dentification, content of their service's system, communication traffic, terminals and any other data required by the National Telecommunication Regulation Authority.

15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

It is recommended or required to consult with the Data Protection Center in the following cases, amongst others:

As a Data subject – in case there has been a breach or violation this individual is recommended and entitled to contact the regulator for the adequate legal consequences to follow the breach.

As a Data Protection Officer – In the case of a breach or violation the officer is responsible for notifying the Data Protection Center. They are also responsible to contact the center with regards to any questions or complaints that individuals may have voiced.

As a data controller or processor – for the application for a license or any other obligations that need to be met as specified by the provisions of the Personal Data Protection Law.

16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

Yes. Article 9 of the PDPL requires the DPO to conduct a periodic examination and evaluation of personal data protection systems. It therefore prevents them from going through documenting the evaluation results and issuing the recommendations for their protection again.

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

Yes, the PDPL, according to Article 8, requires controllers and processors to appoint an employee that is then made responsible for the protection of personal data as the Data Protection Officer. That Data Protection Officer must be registered with the Data Protection Center.

The DPO is responsible for the protection of personal data and the implementation of the data protection Law provisions, its regulations, and the decisions of the DPC. He is also responsible for the supervision of measures implemented within their organization, as well as the handling of requests that are related to personal data under the law.

Article 9 of the Data Protection Law defines the duties of the DPO as follows:

- conduct periodic assessment and evaluation of data protection systems and measures, document the results of such evaluations, and issue recommendations in response to them.
- be the point of contact with the DPC and give effect to its decisions.
- facilitate data subject rights pursuant to the Data Protection Law.
- notify the DPC in the event of a breach of personal data.
- respond to data subject requests and respond to the DPC in relation to any complaints it receives under this law.
- consistently monitor and update personal data records of the controller, or data processing records of the processor, to guarantee the accuracy of the data and

information attached to it.
- eliminate any violations of personal data within their organization, and take the necessary procedures to correct it; and
- organize necessary employee training programs to ensure their competent to give effect to the provisions of the law.

The Executive Regulation, which is yet to be issued, shall specify the obligations, commitments and roles of the Data Protection Officer further.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

Article 9 of the PDPL stipulates that the DPO is required to organize necessary employee training programs to guarantee their competency to give effect to the provisions of the law. The Executive Regulation is to further clarify the obligations of the DPO.

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

Article 2 of the PDPL provides for the data subject's right to be informed of the type of personal data that is being held by the data controller, holder, or processor. The data subject also has the right to know if there is any breach or violation of their data protection rights.

20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Article 1 of the Data Protection Law clearly defines data controllers, data processors and data holder or owner.

Data Holder is any natural or juridic person that legally or has any kinds of personal data in their possession, through any means of storage. The holder can either be the creator of the data or the data has been transferred to them by any means.

Data Controller is any natural or juridic person that has the right, based on the nature of their work, to receive personal data and to determine the process and criteria of retaining or processing that personal data and to control it according to its purpose.

Data Processor is any natural or juridic person that is involved in the processing of personal data for their own benefit or the benefit of the data controller, which is based on an agreement with the data controller and the instructions thereof.

21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

Article 4 of the PDPL states that the measures, methods, and procedures for processing personal data by the controller must all be driven by the specified purpose, unless the processor has been authorized by the controller by means of a written contract.

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

To our understanding, the Data Protection Law does not provide for the above-mentioned rights.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

There are no specific laws or regulations under the Egyptian jurisdiction that restrict targeted advertising or cross-contextual behavioral advertising. The Personal Data Protection Law, which regulates the collection, processing, and transfer of personal data, provides a definition for targeted advertising. The definition under the Personal Data Protection Law states that it is a form of direct marketing that is based on the analysis of personal data with the purpose to reach out to specific

individuals. Under the law, individuals are required to have the option to opt-out of targeted advertising, and businesses must obtain explicit consent by the individual before using any personal data.

Cross-contextual behavioral advertising refers to the collecting of personal data on an individual across several websites, application and other sources for the purpose of creating targeted ads for said individual. The PDPL does not specifically address the matter. However, it would also fall under the definition of targeted advertising.

Article 4 of Law No. 52 of 1981 on the Protection against Smoking forbids government organizations and public institutions, such as sporting clubs and other public entertainment places to participate in the advertising of tobacco and cigarettes. Article 5 further states the complete ban on the advertisement of alcoholic beverages on national TV, national radio and in print media.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or related terms defined, and what restrictions are imposed, if any?

Article 22 of Law No. 175 of 2018 on Anti-cyber and Information Technology Crimes states that the selling of data, amongst other crimes listed, is to be penalized with a minimum of five years of imprisonment and a fine of 300,000 – 500,000 EGP.

25. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Sensitive data and direct online marketing are considered specific regulatory areas under the PDPL. Specific conditions are set out by the law for the handlers to regulate their activities. These activities include the electronic record-keeping of data, in addition to incremental obligations specifically destined for online marketers themselves.

Article 17 of the PDPL prohibits direct marketing by electronic means, such as e-mail and SMS) unless the following conditions are met:

- The consent of the recipient is obtained.
- The identity of the sender is revealed.
- The valid and complete address of the sender is provided.
- There is an indication that the email or SMS is for marketing purposes.
- An opt-out address is provided.

Senders are always obliged to abide by the specified marketing purpose, non-disclosure of the contact information of the person concerned, keep records of the acceptance or non-objection of the recipients for three years as a piece of evidence (Article 18 PDPL).

26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these terms defined, and what restrictions are imposed, if any?

The PDPL does not define "biometrics". However, biometrics may be considered as "sensitive data" in the sense of the PDPL and hence, are expected to be subject to the same protection rules of sensitive personal data protection explained earlier.

27. Is the transfer of personal data or PII outside the jurisdiction restricted? 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? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

Cross-border transfers of Personal Data may only take place if two conditions are met:

1. Data protection in the foreign receiving country must be equally as secure as under the Egyptian Law or even provide for additional requirements. (Article 14)
2. A license for cross-border transfers must be granted by the Center (Article 14).

The PDPL does not provide information on how to assess whether a foreign country meets the requirements. It is expected that the Executive Regulations, once issued, will cover cross-border data transfer requirements in more detail.

However, in limited cases provided under Article 15 of the PDPL and provided that a permit by PDC is obtained,

transferring, sharing, circulating or processing Personal Data may take place without the required minimum data protection level in the foreign country, if the explicit consent of the data subject or his representative is obtained. These cases are the following:

- To preserve the life of the data subject and provide him/her with medical care or treatment or the management of health services.
- To perform obligations in order to ensure that a right is proven, exercised or defended before the judiciary.
- To conclude an agreement or execute an agreement already concluded or, to be concluded, between the processor and third party, for the benefit of the data subject.
- To perform a procedure relating to international judicial cooperation.
- There is legal necessity or obligation to protect the public interest.
- To transfer money to another country pursuant to the laws in force of that country.
- If the transfer or circulation is pursuant to a bilateral or multilateral international agreement to which Egypt is a party.

In addition, under Article 16 of the PDPL, the controller or processor may only disclose or give access to Personal Data to another controller or processor outside the Arab Republic of Egypt by virtue of a license from the PDC, provided that the following conditions are met:

- There is conformity between the nature of work of each of the controllers or processors, or unity of the purpose for which they obtain the Personal Data;
- Each of the controllers, the processors, or the data subject, have a legitimate interest in the Personal Data; and
- the level of legal and technical protection of the Personal Data provided by the controller or the processor abroad shall not be less than the level of protection provided in the Arab Republic of Egypt.

28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Article 7 of the PDPL stipulates that whenever data controllers and data processors become aware of any breach or violation of personal data, they are required to report such to the Data Protection Center within 72 hours. In case the breach or violation is related to national security, they are required to report the violation/ breach immediately. Furthermore, the data controller and processor are to inform the data subject within three days as of the date the breach/ violation was reported to the DPC.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define “security breach”?

Under the PDPL, a security breach is not defined, however Article 7 clearly stipulates the obligation to notify the DPC in case a breach or violation relates to national security.

Article 20 of Law No. 175 of 2018 on Anti-cyber and Information Technology Crimes on cybercrimes related to the State, stipulates that anyone that hacks into the system, or illegally obtains or shares information related the State shall be punished with imprisonment for a minimum of two years and obtain a fine of no less than 100,000 EGP.

Article 1 of Cybersecurity Law defines National Security as anything that relates to the maintenance or establishment of national security, anything that is connected to the national presidency and ministry of defense, national security forces, ministry of defense, ministry of internal affairs, intelligence or the Administrative Control Authority.

30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

Based on the PDPL, the provisions do not specify specific security requirements on individual sectors. However, specific laws related to the respective sectors might provide for some obligations. Please see our answer to question 1 above.

31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice in your jurisdiction?

The PDPL obliges data processors and controllers to inform the Data Protection Center of any breach or violation within 72 hours of the occurrence of said breach/ violation. In case of a breach of national security, the Center is to be informed immediately and accordingly the data subject. Unlike the GDPR, the Personal Data Protection Law requires both the processor and the controller of personal data to notify a breach or violation.

There is also the obligation to notify the National Telecommunication Regulatory Authority of any Cyber-attacks as part of the Anti-Cyber and Technology Crimes Law.

The Executive Regulations of the PDPL that are yet to be issued and implemented, are to clarify the procedures for reporting and notification.

32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the payment of ransoms in ransomware attacks?

Considering the current laws, there are no clear legal requirements or guidance regarding the payment of ransoms in specific. Nevertheless, in 2018 the Egyptian parliament passed Law No. 175 of 2018 on Combating information Technology Crimes, which addresses cybercrimes. Article 27 of said law states that any natural or legal person that uses the internet or any information technology means to commit any crime, shall be punished by imprisonment and a fine ranging from one million to ten million EGP. Accordingly, this provision could be interpreted to apply to those who pay ransoms in response to ransomware attacks.

The Law on Combating Information Technology Crimes also empowers the government to remove or censor any content on in the cyberspace that violates the law or threatens national security. The Egyptian Government also established a National Cybersecurity Center, that is responsible for coordinating efforts to combat cybercrime and improve cybersecurity across the State.

33. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

A dedicated police department (which is a wing of the Ministry of Interior) is entrusted with the detection and investigation of internet crimes. A lot of these crimes, by their very nature, include the breach of personal data and accordingly, might overlap with the PDPL.

34. Do the laws in your jurisdiction provide individual data privacy rights such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Yes, there are several individual data privacy rights set out by the PDPL including the following:

- Right to be informed (Article 2) – the data subject has the right to be informed of the type of personal data that is being held by the data controller/ holder/ processor. The data subject also has the right to be informed of any breach of violation of their data protection rights.
- Right to access (Article 2) – the data subject's right to access or obtain personal data held by the data processor/ holder/ controller.
- Right to rectification (Article 2) – provides the data subject with the right to amend their personal data.
- Right to erasure (Article 2) – gives the data subject the right to delete any of their personal data.
- Right to object (Article 2) – the data subject has the right to object to the processing of personal data whenever it collides with the fundamental rights and freedoms of the data subject themselves. The data subject also has the right to revoke the consent that they granted for the storing or processing of personal data. The data subject may also refuse the electronic communication or electronic marketing of personal data (Article 17).

35. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Individual data privacy rights are exercisable through both the judicial system and enforced by a regulator (i.e., Data Protection Center). According to Article 19 of the PDPL, the Data Protection Center is empowered to oversee and enforce the PDPL. The Data Protection Center is however not yet operational.

36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

According to Article 33 of the PDPL, the person concerned or of capacity who has a direct interest shall have the right to recourse to court or to lodge a complaint in the following cases:

- The violation of personal data protection rights
- The prevention of the person concerned from satisfying their rights.
- The resolutions issued by personal data protection officer at the processor or controller, regarding requests submitted thereto.

The complaint shall then be submitted to the DPC, that will issue its decision within thirty days of the submission of the complaint. The respondent shall then implement the Center's decision within seven working days of having been notified of the decision.

The Executive Regulation is to further clarify the enforcement mechanisms of the PDPL.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

Yes, an injured individual may be entitled to damages under the general principles of tortious liability provided in the Civil Code. The Civil Code requires that the injured establishes the elements of (i) fault, (ii) damage and (iii) a causal link. Emotional damage is adjudicated in limited cases but still needs to be established. We are not aware of judicial precedents of emotional damages awarded specifically as a result of violation of the PDPL or the Cybersecurity law, noting however that both laws are quite novel and have not yet been enforced to their full extent.

38. How are data protection, privacy and cybersecurity laws enforced?

The main regulatory authority of the PDPL is the Data Protection Center is responsible for the enforcement of the Personal Data Protection Law. It is unclear how the data protection is to be enforced as the Executive Regulation is yet to be issued and accordingly the Data Protection Center is not yet operational.

For cybersecurity enforcement, the internet investigations police department are responsible for the enforcement of Cybercrime Law and receives complaints by citizens. Said police division is responsible for all crimes committed through the internet, which therefore includes crimes involving personal data breaches.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

The Cybercrime Law penalizes violations of the cybercrime regulations by imposing various penalties on the violators, which include fines, imprisonment, and censorship of content. Sanctions can therefore include administrative fines (up to EGP five million) as well as criminal penalties (imprisonment of more than six months).

The PDPL criminalizes personal data breaches and consequently imposes fines with a sum of up to five million EGP for violators of the law.

Some of the key offences and their sanctions include the following:

- Article 36: The unlawful disclosure of personal data, result in a fine of between 100,000 and 1 million (EGP). If the disclosure is for the purpose of a moral benefit at the expense of the data subject, the fine will be doubled, and a prison sentence of a minimum f six months will be imposed. If the disclosure involves sensitive data, the fines range between 500,000 and 5 million EGP and a minimum of three months' imprisonment shall follow.
- Article 40: The failure to appoint a Data Protection Officer or the failure by a Data Protection Officer to meet their obligations results in a fine between 200,000 and 2 million EGP.
- Article 42: The violation of a cross-border transfer requirement results in a fine between 500,000 and 5 million EGP and a minimum of three months' imprisonment. The violation of the electronic marketing rules results in a fine of 200,000 to 2 million EGP.

40. Are there any guidelines or rules published regarding the calculation of fines

or thresholds for the imposition of sanctions?

The thresholds of penalties for each type of violation are provided in the law. These, however, are provided as a minimum or maximum. Deciding on the exact penalty within the provided range is expected to fall within the court's discretion.

41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Yes, personal data owners should be able to appeal to the courts against orders of the regulators under the general rules of the administrative law.

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

It is still not possible to identify trends in enforcement regarding the PDPL given that the Executive Regulation is not yet issued and the DPC is not yet operating.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

As explained earlier, the issuance of the Executive Regulation is yet to take place, which will expand on the provisions of the newly published PDPL and further clarify the procedures and actions associated with some issues such as cross-border data transfers. As a result, calls and proposal for any reform are, in our view, premature.

Contributors

Dr. Ingy Rasekh
Managing Partner (Cairo)
rasekh@amereller.com

Nisreen Al-Karyouti
Partner (Cairo)
karyouti@amereller.com