Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Egypt: Law & Practice

Nevine El-Shafei, Tasneem El-Naggar and Dina El-Saiedi
Shehata & Partners

practiceguides.chambers.com

EGYPT

Law and Practice

Contributed by:
Nevine El-Shafei, Tasneem El-Naggar and Dina El-Saiedi
Shehata & Partners see p.33

Contents

1. Basic National Regime

1.1 Laws

The Data Protection Law and the Telecommunications Law

The revolution in the field of communication technology, and the increasing reliance on it by governments and individuals, is unfortunately also associated with increased risk in its use in various sectors. Against this background, it has become necessary to create an appropriate legal landscape to protect data and privacy in information technology and communication as part of its targeted economic growth. To advance this protection in the informational technology field, Egypt issued the Data Protection Law No 151/2020 (DPL) in 2020, which encompasses the protection of individuals' and entities' data and privacy rights. The DPL generally prohibits the processing of personal data without the explicit consent of data subjects and, in addition, grants them multiple rights in restricting access to their data, withdrawing their prior consent, and informing them in the case of any data violation.

Generally, the right to privacy is at heart of the freedom rights established under the Egyptian constitution. In addition, a number of laws recognise the right to privacy, such as, the Penal Code in Telecommunications Law No 10/2003 (the "Telecommunications Law"). See **2.5 Enforcement and Litigation**.

On the other hand, sensitive and emerging technologies, such as AI, are advanced technologies that include multi-layered interactions and services that require the collection of enormous amounts of personal data. Such advanced technologies are therefore generally subject to the DPL and the Telecommunications Law, which is a more specific law, relevant to such technologies.

Under the DPL, in principle, any digitally collected and/or processed data must meet the following conditions (the "General Conditions"):

- personal data will be collected for the legitimate, specific and declared purposes of the person concerned;
- collected data must be true, sound and secure;
- collected data must be processed in a manner that is lawful and appropriate to the purposes for which it was compiled; and
- collected data must not be kept for longer than the period necessary to fulfil the purpose specified for it.

The IoT Framework of the National Telecommunication Regulatory Authority

The technology of the Internet of Things (IoT) mainly depends on the collection of data and its exchange, analysis and processing. Therefore, an IoT service provider is obliged to take all necessary institutional and technical procedures and steps to protect the confidentiality of information and data of the service users, as per the general obligations prescribed by the framework issued by the relevant authority, ie, the IoT Framework of the National Telecommunication Regulatory Authority (NTRA). Furthermore, it is explicitly stated under the same framework that the IoT Framework is subject to the provisions of the Telecommunications Law and, in particular, the DPL as stated above in relation to AI technology.

The Cybercrimes Law

In addition, the Cybercrimes Law No 175/2018 on combating IT crimes (the "Cybercrimes Law"), and its executive regulation No 1699/2020, regu-

late online activities and aim to penalise, inter alia, unlicensed online activity and content violations, such as illegally accessing a private device or account, a very possible crime under sensitive digital technologies.

Service providers under the Cybercrimes Law have a number of obligations that, to a great extent, protect service users, such as:

- keeping and storing the record of the information system or any means of IT, for a continuous period of 180 days;
- maintaining the confidentiality of the data that has been saved and stored;
- not disclosing the data without a justified order from a competent judicial authority; and
- securing data and information in a manner that preserves its confidentiality, and does not penetrate or damage it, etc.

In addition, service providers are also required to undertake technical and control measures to prevent cyber-attacks and safeguard the security of the technology and information system, such as, encryption, multi-factor authentication, and other security alerts.

Other Regulations

Fundamental privacy and data protection provisions to regulate sensitive digital technologies and penalise infringements are further specified in a number of dispersed regulations, which apply whenever they are applicable to the case in hand, such as the following.

- Law No 58/1937 issuing the Criminal Law, as amended, (the "Penal Code") – Articles 309 (bis) and 309 bis (A) penalise invasion of privacy and obtaining and disclosing personal information without lawful means.
- Law No 15/2004 regulating e-signatures and establishing ITIDA and its executive regulations – Article (13) provides that applicants to e-signature services must ensure, inter alia, (i) a secured system to preserve the secrecy and privacy of the information as per legal standards, and (ii) a system to preserve the confidentiality of information relating to the performance of licensed services and customers' data.
- Decree No 667/2017 by the Minister of Telecommunications and Information Technology issuing the contravention and penalty regulations on communication service providers – generally, these regulations set out penalties to be applied when telecommunication service providers breach regulations by the NTRA issued in connection with users' rights protection. Also, these same regulations penalise telecommunications service providers for infringing the data privacy requirements provided in the service provider's licence.
- NTRA regulations in connection with obtaining a communication licence and providing communications services in Egypt.
- NTRA general rules in connection with protecting internet users' rights – Article (12) provides the duty of the communication service provider to preserve the secrecy of customers' information and not to disclose such information except in the cases permitted by law.
- NTRA general rules in connection with protecting mobile and telephone users – Article (22) provides the duty of communication service providers to preserve the secrecy of customers' information and not to disclose such information except in cases permitted by law.
- NTRA guidelines on consumers' rights and obligations.

1.2 Regulators

Data Protection Key Regulators and Their Respective Areas of Jurisdiction

The DPL has identified data privacy and protection's key regulator and its respective area of jurisdiction in the heart of Article (19), where it is stated that a Data Protection Centre (DPC) will be established to protect personal data and organise its processing and availability. In order to achieve its objectives, the DPC may exercise all the competencies stipulated in the DPL, including the following:

- setting and developing policies;
- implementing decrees and procedures for the protection of personal data;
- unifying data protection and processing policies;
- co-ordinating with all government and non-government authorities to ensure the application of personal data measures;
- issuing licences, approvals and various measures related to the protection of personal data;
- receiving complaints related to the application of the DPL to issue the necessary decisions in this regard;
- monitoring those addressed by the DPL and taking the necessary legal measures;
- checking the conditions for cross-border data movement;
- concluding agreements and memorandums of understanding, co-operating, and exchanging experiences with the relevant international bodies; and
- preparing an annual report on the status of personal data protection in Egypt.

Unfortunately, at the time of drafting this article, the DPC had not yet been established. It is expected that the authorities concerned will expedite its establishment sooner or later, due to the important role the DPC will play in implementing the DPL provisions.

Data Protection Centre Judicial Authority

The 13th and 14th chapters of the DPL grant the status of judicial officers to the employees of the DPC and prescribe penalties for violating the provisions of the DPL, in addition to regulating the methods of reconciliation when any of these violations are committed.

For instance, a fine of not less than EGP100 thousand and not exceeding EGP1 million, will be charged to any data controller, processor, or holder who discloses personal data or who makes it available, in cases other than those punishable by law. A controller or processor who prevents the person concerned with the data from exercising the rights conferred upon them by law, will be punished with the same penalty. Furthermore, the penalty is increased to a fine from EGP500,000 to EGP5 million where violating the provisions of permits or licences should be pursued under the DPL.

It is worth mentioning that the DPL has adopted a relatively new punitive act which penalises those responsible for the actual management of a legal person with the same penalties prescribed for individuals violating the provisions of the DPL, if it can be proved that the manager was aware of such violations and that breach of their duties contributed to the occurrence.

1.3 Administration and Enforcement Process

Practically speaking, there are still no precedents in relation to the administrative process that the DPC must follow to investigate and impose penalties on DPL violators, due to the fact that the DPC has not yet been established, along with the absence of DPL executive regulations that

should regulate such administrative process. Nonetheless, the DPL states that any person concerned about personal data, who has capacity and direct interest, has the right to complain to the DPC in the following cases, without prejudice to the right to resort to the judiciary (also see **2.5 Enforcement and Litigation**):

- violation or breach of the right to protect personal data;
- the person concerned is prevented from fulfilling their rights; and
- regarding decisions issued by the DPO in connection with requests submitted to it.

The complaint will be submitted to the DPC, which will follow the necessary investigation procedures. The DPC must issue its decision within 30 working days from the date of the submission, provided that the complainant and the defendant are notified of the decision.

The defendant is obliged to implement the DPC's decision within seven working days from the date of notification, and to inform the DPC of what has been done towards the implementation of its decision.

1.4 Multilateral and Subnational Issues

The main intention of the authorities issuing the DPL was to keep pace with current developments in the field of communication technology, and to protect the right to privacy. The DPL adopts the European Union General Data Protection Regulation (GDPR), with the addition of amendments and standards that contribute to enhancing the protection of personal data and privacy.

Principles Adopted From the GDPR

The DPL has adopted several principles from the GDPR including the following.

The DPL outlines a list of definitions for data protection that are binding and included in the legal framework

According to this principle, the law must contain clear concepts for personal data and sensitive personal data and include the procedures followed to protect personal data during communications, which preserves the privacy of those communications and the privacy of the data that is exchanged.

The DPL has provided clear definitions of personal data and sensitive personal data, as well as a definition of the holder of information and the processor, and seeks to preserve the right of the data subject, whether the processor is represented by an individual or a company. This is done by criminalising, for instance, the use of data without the knowledge of its owner or intransigence in enabling the owner of the data to have the right to view it.

The DPL determines the legal basis that allows the data to be processed

This principle obliges the law to define a legal basis for any entity that processes personal data to guarantee its safety before the law by implementing the terms of the contract according to the user's consent, as well as the user's rights, such as giving the user the right to withdraw consent. In this regard, Article (2) of the DPL guarantees "the right to withdraw prior consent to the retention or processing of personal data".

The DPL includes a list of users' rights that are binding under the law

This principle guarantees users' rights and control over their data, such as the right of objection, erasure, correction, the right to receive information, and the right to enquire. The DPL guarantees all these rights, but sets a fee for exercising these rights, with the exception of the right to

enquire in the event of personal data violation. The fee may not exceed EGP20,000, where the DPC is responsible for issuing decisions related to determining and receiving financial compensation.

The DPL outlines a clear scope of application
The DPL clarifies in Article (2) the scope of its application, including anyone who commits one of the specified crimes under the DPL, and who is (a) an Egyptian, whether present in Egypt or residing abroad, or (b) a non-Egyptian residing inside Egypt, or (c) a non-Egyptian residing abroad, if the act is punishable in the country in which it occurred under any legal description, and the violated data belongs to Egyptians or foreigners residing inside Egypt.

The DPL establishes binding and transparent mechanisms for the secure transfer of data to other countries
The DPL prohibits transferring data across borders, whether by collecting, storing, processing, or sharing, with a foreign country that does not provide the same level of protection stipulated under the DPL.

Given the above-mentioned, one could say that the DPL greatly relates to the multinational principles of the GDPR; however, the DPL has several shortcomings represented by the failure to rely on the involvement of the various groups of society in drafting and preparing the law. It is still possible to address these shortcomings with the issuance of the DPL executive regulations, in the hope that the authorities will be aware of current developments in the electronic world in a way that protects and promotes privacy and data protection rights.

1.5 Major NGOs and Self-Regulatory Organisations

Generally, NGOs and SROs must comply with the data protection standards and regulations stipulated under the DPL, due to the fact that they are legal entities that have a juristic personality. In this regard, Article (8) of the DPL obliges the legal representative of a legal entity that controls or processes personal data to appoint, within the legal entity and functional structure, a data protection officer (DPO) responsible for the protection of personal data. This DPO must be registered in a special register to be established at the DPC.

The DPO is responsible for implementing the provisions of the DPL, its executive regulations, and the decisions of the DPC, monitoring the procedures in force within their entity, supervising them, and receiving requests related to personal data in accordance with the provisions of the DPL.

In particular, a DPO is committed to the following:

- conducting periodic evaluation and examination of personal data protection systems and preventing their penetration, documenting evaluation results, and issuing the necessary recommendations to protect them;
- acting as a direct point of contact with the DPC and implementing its decisions with regard to the application of the provisions of the DPL;
- enabling the person concerned with the data to exercise their rights as stipulated in the DPL;
- notifying the DPC in the event of any breach or violation of its personal data;
- responding to requests submitted by the person concerned with the data or anyone

with this capacity, and responding to the DPC in the grievances submitted to it by any of the persons concerned, in accordance with the provisions of the DPL;
- following up with the registration and updating of the controller's personal data record or the processor's processing operations record, to ensure the accuracy of the data and information entered therein;
- removing any violations related to personal data within the entity, and taking corrective measures in this regard; and
- organising the necessary training programmes for the entity's employees, to qualify them in accordance with the requirements of the DPL.

In addition, NGOs and SROs may create their own data protection policies, as the DPL does not prevent legal entities from developing their own internal policies. However, such internal policies may not contradict the provisions of the DPL.

1.6 System Characteristics

Due to the fact that the DPL was recently introduced to Egyptian society, the procedural aspect is still unclear. Although the DPL greatly relates to the multinational principles of the GDPR, it has several shortcomings, such as failure to rely on the involvement of the various groups of society in drafting and preparing the law. It is still possible to address these shortcomings with the issuance of the DPL executive regulations and with the establishment of the DPC, in the hope that the authorities will be aware of current developments in the electronic world in a way that promotes privacy and data protection rights.

1.7 Key Developments

Egypt recently introduced the DPL. This is considered a key development in Egyptian society, as the revolution in the field of technology and increasing reliance on it by governments and individuals in Egypt, has increased the risks associated with the use of communication technology, especially the risk of violating the right to privacy.

Nevertheless, the executive regulations for the DPL have not yet been issued, even though these should have been issued within six months of the date on which the DPL came into force. Furthermore, the awaited DPC has not yet been established, which leaves a great deal of room for the DPL to be interpreted by the issuance of its executive regulations and the establishment of the DPC.

1.8 Significant Pending Changes, Hot Topics and Issues

The current main hot topic in connection with data protection is probably the DPL executive regulations, which are now long awaited. The enactment of the DPL executive regulations will indeed determine the procedural application pertaining to data protection and its underlying activities. Also, it is key to effectuate the incorporation of the DPC, in order to realise the regulatory and procedural application of the DPL. In practice, many companies, especially online platforms, rely on self-assessment schemes (eg, adding privacy and data protection policies). This primarily stems from being aware of the ongoing need to meet global business and market standards, which heavily encourage data protection and privacy. It is indeed both a legal and social necessity to have in place a proper regulatory and procedural framework to protect privacy and personal data, which is a funda-

mental right, and to provide adequate means of enforcement in the Egyptian market.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The DPL generally applies to personal data collected, controlled or processed digitally. Personal data is defined under the DPL as: "Any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking such personal data and other data such as name, voice, picture, identification number, internet identifier, or any data which identifies the psychological, medical, economic, cultural, or social status of a natural person."

A data subject is defined as "any natural person to whom electronically processed personal data is attributed which establishes his/her legal or factual identification and enables his/her identification from any other person".

In addition, data possessor means "any natural or juristic person [who], legally or factually, holds and retains personal data in any manner, or by any means of storage, regardless of whether that person initially created such personal data or [it] was transferred to such person by any means".

Data processor is also defined under the DPL as "any natural or juristic person, specialised due to the nature of their work activity, to process personal data for their own benefit or for the benefit of the data controller as agreed with and instructed by the data controller".

The DPL deals with the protection of personal data from rights and obligations standpoints. The rights are those conferred to the data subject who owns the personal data (see "Rights" in **2.5 Enforcement and Litigation**). On the other hand, the obligations are those of the data controller, data processor, and data possessor (whether they are natural or juristic persons). The collection, retention and processing of personal data pursuant to the DPL should generally be carried out in accordance with the following conditions:

- for a legitimate, specific purpose notified to the data subject;
- the personal data should be correct, accurate and secured;
- the personal data should be processed lawfully and in conformity with the purpose of its collection; and
- the personal data should not be kept for a period exceeding the time required for it to fulfil its purpose.

The DPL excludes a number of activities that are dealt with under special laws or statutes (see "Excluded Activities" in **2.5 Enforcement and Litigation**). Although the DPL provides an umbrella framework pertaining to the use and processing of personal data (with the exception of "Excluded Activities"), some sectoral legislation is in place to deal with the matter of privacy and the use of personal data separately. This is illustrated, for example, in the Fintech Law, the Telecommunications Law, and the Consumer Protection Law. The general requirements in connection with data processing and control are set out below.

Data Processing

Definition

Under the DPL, data processing refers to "any electronic or technical means to write, collect, record, save, store, merge, display, send, receive, circulate, publish, erase, change, edit,

retrieve, or analyse personal data by way of using medium or electronic or technological equipment, whether fully or partially".

Obligations

In addition to the General Conditions, Article (5) of the DPL sets out the data processor obligations, as follows.

- To conduct and implement data processing pursuant to the DPL (and its executive regulations) in accordance with legitimate and legal cases (see "General Conditions" referred to in **1.1 Laws**), and based on the written instructions received from the DPC, the data controller or from any relevant person as applicable. In particular, with due regard to the scope, subject and nature of the data processing and the type of personal data, and its conformity and sufficiency with the designated purpose.
- To ensure the legitimacy of the purpose of the data processing and the practice thereof and the non-violation of public order or morals.
- To not exceed the purpose and period required for data processing, and to notify the controller, the data subject, or each relevant person, as the case may be, of the period necessary for the data processing.
- To delete the personal data following the lapse of the period for processing or to deliver the same to the data controller.
- To undertake or refrain from undertaking an action, which would result in disclosing the personal data or disclosing the outcome of the data processing, except in the cases permitted by law.
- Not to undertake any processing of personal data that contradicts the purpose or the activity of the data controller unless such processing is for a statistical or educational purpose that is non-profit and without prejudice to the inviolability of private life.
- To protect and secure the processing activity and the mediums and the electronic devices used in processing, as well as the personal data thereon.
- Not to cause harm, whether directly or indirectly, to the data subject.
- To prepare a special record to capture the data processing activities, provided that it includes the processing categories undertaken on behalf of any data controller, its contact details, its DPO, the period, restrictions and scope of data processing, the mechanisms for deleting or modifying the personal data, and a description of the technical and organisational procedures related to the data security and the data processing activities.
- To provide the means to prove the data processor's compliance with the provisions of the DPL, at the request of the data controller, and to enable the DPC to conduct inspections and supervision to ensure compliance with the provisions of the DPL.
- To obtain a licence or permit from the DPC in order to handle personal data.
- To appoint a local representative when the data processor is outside the Arab Republic of Egypt. The appointment must be made in accordance with the DPL executive regulations.

Legitimate processing

In addition to the above, Article (6) of the DPL provides criteria for the legitimate and lawful conduct of the processing of personal data ("legitimate processing"), as follows:

- the consent of the data subject on effecting the data processing for a given purpose(s) must be obtained; and
- the data processing must be necessary and imperative to comply with a contractual obligation, legal act, concluding a contract

in favour of the data subject, or undertaking procedures to claim or defend legal rights; or
- the data processing must be required to implement a legal duty obliged by law or to effectuate an order from a concerned investigation authority or a court judgment.

Data Control

Data control activity is not defined per se under the DPL as separate to data processing. However, the DPL includes data control within the activities of the data controller. The data controller is thus defined as "any natural or juristic person who has – by virtue of the nature of their activities – the right to obtain personal data and to specify the method and criteria of keeping, processing or controlling such data in accordance with the specific purpose or [otherwise aligned] with the data controller's activities."

Data controller's obligations

In addition to the General Conditions, Article (4) of the DPL sets out the data controller's obligations, as follows.

- To obtain or receive personal data from the data holder or the competent entities which provide such data, as the case may be, after obtaining the data subject's consent or unless otherwise permitted by law.
- To ensure the validity, conformity and sufficiency of the personal data with the purpose of its collection.
- To set the method, manner and standards for data processing pursuant to the designated purpose, unless it has been decided that the data processor should decide on the above by virtue of a written agreement.
- To ensure the purpose pertaining to the collection of the personal data meets the data processing objectives.
- To undertake or refrain from undertaking an action which would result in disclosing personal data, except in cases permitted by law.
- To adopt all technical and regulatory procedures and apply the necessary standard criteria for protecting personal data and ensuring its confidentiality, and preventing any hack, damage, alteration or manipulation through any illegitimate process.
- To delete any personal data in the data controller's possession upon the satisfaction of the designated purpose. However, in the case of retention of such data for any legitimate reason after the satisfaction of its designated purpose, the data shall be retained in a form that does not allow the identification of the data subject.
- To correct any error in the personal data immediately upon being notified or becoming aware of such error.
- To maintain records of personal data, provided that this includes a description of the categories of personal data in the data controller's possession, determining the persons to whom such data may be disclosed or made available, along with the basis, duration, restrictions, and scope thereof, as well as mechanisms to delete or modify the personal data, or any other relevant data related to cross-border personal data transfer. The record must also include a description of the technical and regulatory procedures for maintaining the security of the personal data.
- To obtain a licence or permit from the DPC to handle personal data.
- Where the data controller is outside the Arab Republic of Egypt, to appoint a local representative in accordance with the DPL executive regulations.
- To provide the necessary means to establish observance of the DPL and to enable the

DPC to conduct inspections and supervision to ensure the same.

Duty to Report

Article (7) of the DPL requires the data controller and the data processor to report to and inform the DPC of any breach or violation of the personal data within 72 hours from the time of becoming aware of such breach or violation (see **2.5 Enforcement and Litigation**). If such breach or violation represents national security concerns, the reporting to the DPC should be made immediately and the DPC should also immediately inform the concerned national security authorities of the incident. The data controller and data processor (as applicable) should also supply the DPC with the following information:

- the nature of the breach or violation, the type, reasons and estimated number of personal data records;
- the details of the DPO;
- the possible consequences of the breach or violation; and
- a description of the procedures undertaken.

Data Protection Officer

Article (8) of the DPL provides that the data controller or data processor is required to appoint a DPO. Corporate entities carrying out data control or data processing activities are required to appoint a DPO within their legal and employment structure and register the DPO with the DPC. The DPO registration requirements will be set out in the DPL executive regulations.

The responsibilities of the DPO will include:

- observing application of and compliance with the DPL (and its executive regulations);
- regularly evaluating and inspecting the data protection systems to avoid any breach;
- registering the outcome of this evaluation and issuing the necessary recommendations;
- acting as a direct point of contact with the DPC and applying the DPC decisions in connection with the DPL application;
- notifying the DPC of any violation of the personal data;
- responding to any request made by the data subject or authorised third party;
- responding to any grievance submitted to the DPC by the data subject or authorised third party, pursuant to the DPL;
- following up on the registration and update of personal data and carrying out relevant corrections in this respect; and
- arranging training and compliance sessions for the employees (of the data processor or data controller).

Other Key Considerations

Data protection and privacy, while mainly subject to the DPL from a technological standpoint, is deemed a fundamental right under various other legislations such as, the Telecommunications Law, the Consumer Protection Law, the E-signature Law, and the Banking Law. These are discussed in **2.2 Sectoral and Special Issues**.

2.2 Sectoral and Special Issues

Refer to **2.5 Enforcement and Litigation** in connection with data subject rights. In addition to this litigation, a number of laws also regulate the matter of privacy and data protection from a sectoral/activity standpoint.

Sensitive Data

The DPL defines “sensitive data” as “data disclosing the psychological, mental, physical or genetic status, or biometric or financial data, religious beliefs, political views, or criminal records. In all cases, data relating to children

is considered to be sensitive personal data". The collection or processing of sensitive data requires a prior licence from the DPC in addition to the consent of the data subject (except in cases permitted by law). The means of protecting sensitive data, including policies and security procedures in this respect, is decided in the DPL executive regulations. Breaching of sensitive data requirements under the DPL will result in a minimum prison sentence of three months and/or a monetary fine ranging between EGP500,000 and EGP5 million.

Financial Data

The DPL classifies financial data as sensitive data. Consequently, both banking and fintech laws also set out the obligation to protect customers' data, which is recognised as a fundamental right of customers in the finance sector. The finance sector, pursuant to Egyptian law, is dealt with under Banking Law No 194 for 2020 (the "Banking Law") and Fintech Law No 5 of 2022 (the "Fintech Law"). The Banking Law deals with banking activities such as accepting deposits, opening accounts, money remittances, payment services, and granting loans ("Banking Activities"), and the Fintech Law deals with non-banking financial activities using technology ("Fintech Activities"). Fintech Activities are regulated and supervised by the Financial Regulatory Authority (FRA).

For instance, Article (140) of the Banking Law provides that all customers' data, accounts, deposits, safes and transactions related thereto ("Customers' Data"), must be kept confidential and may not be disclosed by any means, whether directly or indirectly, except with the prior written permission of the customer (or their authorised representative) or by way of a court or arbitration order (as applicable). This confidentiality duty will survive even if the relationship with the customer has ended.

In addition, Article (198) of the Banking Law provides the obligation for digital payment service providers to have adequate means in place to protect the electronic systems used against any breach or unauthorised access, cyber-attack, data manipulation, or violation of data secrecy of customers.

Banking activities are among the "excluded activities" under the DPL. The secrecy and protection mean required for customer data in Banking Activities is therefore subject to the regulations and supervision of the Central Bank of Egypt (CBE). Complaints relating to banking services, including breach or violation of customer data, should be reported to a special committee (customers' protection committee) with the CBE.

On the other hand, and without prejudice to the DPL, the Fintech Law also upholds fintech service providers' duty to protect the secrecy of their customers' data (or their customers' transactions) and not to disclose this information, except with the prior consent of the customer concerned (Article 113).

Health Data

Similarly, health data is classified as sensitive data pursuant to the DPL. In addition to the DPL, other legislation deals with privacy and data protection in the health and medicine sector, as follows.

Penal Code

Article 310 of the Penal Code provides that doctors and pharmacists who know secrets, by reason of their profession, then disclose these secrets, are sanctioned by a prison sentence or fine. This also applies to any public official.

Blood Operations Law No 8 of 2021
Article (16) of the Blood Operations Law provides that all entities working in the field of blood operations and plasma collection are under obligation to preserve the confidentiality of the data and not disclose this information, except with a judicial or prosecutor's order. In addition, Article (21) of the Blood Operations Law provides that breaching of this confidentiality duty will result in a monetary fine ranging between EGP100,000 and EGP1 million.

Psychiatry Law No 71 of 2009, as amended, and its executive regulations
Article (4) of the Psychiatry Law provides that psychiatric institutions must prepare a special record of all admitted psychiatric patients. This record includes the data of each patient and must be kept in confidence. Access to this record is permitted to the national mental health council and the established governorate councils for mental health. Access to these records shall be without prejudice to the secrecy of the data. This record should be kept by the institutions concerned for a period of 15 years.

In addition, Article 36 (9) of the Psychiatry Law provides for the psychiatric patient's right to confidentiality and to the protection of their medical records, which may not be disclosed for non-medical reasons, except in cases permitted by law.

Persons with Disabilities Law No 10 of 2018
Article (6) of the Persons with Disabilities Law provides that the Ministry of Health, in co-operation with the Ministry of Social Solidarity, will build a database and protect the privacy of persons with disabilities. This database is used to plan, implement and follow up on the provision of various health services, taking into account the confidentiality of its data.

Additionally, Article (53) of the Persons with Disabilities Law provides that anyone who displays, publishes or broadcasts, by any means of publication, any of the data or information that would offend persons with disabilities, or expose them, will be punished with a fine.

Medical Charter issued by Decree of the Minister of Health and Population No 238 of 2003, issuing charter of ethics and honour in the medical profession
Article (30) of the Medical Charter provides that a doctor may not disclose information relating to their patients except in cases permitted by law.

E-signature Law No 15 of 2004
Article (21) of the E-signature Law No 15 of 2004 and its executive regulations issued by Ministerial Decree No 109 of 2005, as amended, provides that e-signature data, electronic mediums and data submitted to licensed e-signature service providers are confidential, and may not be disclosed or used except within the purposes for which the data was submitted. Also, Article (13) of the E-Signature Law executive regulations provides the licensing requirements for an e-signature service provider which include having in place an adequate system to protect the confidentiality of information relating to the licensed services and to protecting the customers' data.

Consumer Protection Law No 181
Article (29) of the Consumer Protection Law No 181 of 2018 and its executive regulations issued by way of Prime Minister's Decree No 822 of 2019 generally sets out the obligation of a supplier, when concluding a contract with a consumer, to preserve the data and information of that customer without their consent, and not to disclose or share this information in breach of the applicable laws. The supplier is also required

to undertake all the necessary measures to protect and respect the privacy of the customer's data and information.

Telecommunications Law

See also **2.5 Enforcement and Litigation**. The NTRA has issued the telecommunications users' rights guidelines which encompass the obligation of the licensed telecommunications service providers, and their staff, to protect the confidentiality of the users' data and privacy, and not to disclose such information or data, except if required by the law, judicial warrant or by way of the user's consent (by separate signature). Also, these guidelines require licensed telecommunications service providers to have internal procedures in place to protect and secure the confidentiality of telecommunications and telephone conversations made via the network. This includes the protection of confidentiality, and the prevention of wiretapping, recording, broadcasting or publishing of telephone calls (except in response to legal requisites).

2.3 Online Marketing

Generally, Article (17) of the DPL prohibits direct electronic marketing to data subjects, except under the following conditions:

- the approval of the data subject has been obtained;
- the communication includes the identity of the sender;
- the sender can be reached by a valid and complete address;
- reference is made in the communication that it is for direct marketing purposes; and
- clear and uncomplicated mechanisms have been set up to allow the data subject to opt out or withdraw their consent to sending.

In addition, Article (18) of the DPL obliges the sender of direct marketing communication to:

- specify the marketing purpose;
- not disclose the communication information to the data subject;
- keep an electronic registry evidencing the approval of the data subject (as amended), or the data subject's non-objection to proceed, on receiving the direct marketing communication (this registry should be kept for three years from the date of final sending).

The procedures and other requirements in connection with direct electronic marketing are provided in the DPL executive regulations.

In addition to the above, the Consumer Protection Law regulates the way of contracting in the process of displaying, selling or buying products through the internet, or any means of visual, audio or written communication, or by telephone or any other means, ("remote contracting"), where the consumers' rights are upheld to the greatest extent. For instance, if the consumer expresses their acceptance of remote contracting, they have the right to correct or amend their request within seven working days of acceptance, unless the parties agree on a longer period.

2.4 Workplace Privacy

Egypt has undergone a series of legislative changes in recent years, aiming to establish organisational and procedural guidelines for technological advancements and to increase the use of information technology by both individuals and businesses in the workplace. Therefore, employers must be aware of their data privacy responsibilities and liabilities, as they must manage data responsibly and keep up to date with data protection regulations. As a general

rule, employers must be transparent about how they are using and safeguarding their employees' personal data, both inside and outside the workplace.

Laws and Regulations

Prior to the enactment of the DPL, personal data was governed by the general principles of law, such as the Cybercrimes Law and the constitution, protecting the individual's privacy and imposing restrictions on the use and disclosure of data. However, since the issuance of the DPL, employees should understand their rights and responsibilities under this recent legislation, in addition to the employers' need to have adequate data protection policies and procedures in the workplace.

The DPL requires that data controllers and processors establish a lawful basis for each and every personal data processing activity they perform directly or which is disclosed or revealed by any means, except with the explicit consent of the data subject. In addition, each company has to hire a DPO, who will be liable and responsible for any breach to the provisions of the DPL.

The Ability to Monitor Workplace Communications and Any Constraints, Including with Respect to Implementation of Cybersecurity Tools and Insider Threat Detection and Prevention Programmes

The monitoring of employees' activities in the workplace is a sensitive process that could implicate privacy rights, and until now, no specific law enacted in Egypt has specifically dealt with the use and installation of surveillance cameras in the workplace. Before the issuance of the executive regulations of the DPL and the establishment of the DPC, employers tended, in practice, to inform their employees (eg, via email) and could obtain the prior express approval of each data subject to encroach on their privacy by using surveillance cameras for security reasons at the employer's premises.

In this regard, the constitution states that all correspondence, telephone calls, emails, and other forms of communication are protected, and their confidentiality is guaranteed. They may not be confiscated or monitored except by a judicial order, and for a limited time, in accordance with the provisions of the law. Therefore, an employer may not monitor employees' correspondence, as long as it belongs to the employee(s) and is not the employer's property. Moreover, Egyptian Labour Law No 12 for 2003 (the "Labour Law") obliges the employer to collect and receive all possible identifiable information and documents only in connection with the employee's application for employment. In addition, the executive regulations of Civil Service Law No 81 for 2016 (the "ER of the Civil Service Law" state under Article (3) that an electronic or paper file or both, must be created for each employee at the relevant authority, in which documents, data and information only related to the employee's job, notes related to their work, and performance evaluation reports can be deposited. Hence, the DPL, the Labour Law and the Civil Service Law regulate employees' personal information and the mechanism for processing and controlling it, where only work-related data should be collected and monitored.

The Role of Labour Organisations or Work Councils

The new Labour Organisations Law No 213 of 2017 (the "Labour Organisations Law"), which replaced Labour Organisation Law No 35 of 1975, specified the role of labour organisations and work councils that aim to protect employees' rights and resolve their problems. Currently, these labour organisations have the upper hand

in governing all employees' rights and requirements to work in a stable and equitable environment. In addition, these organisations provide an equal platform where the employer and the employee can engage in discussions to solve some of the common problems in the workplace, including the issue of workplace privacy.

Whistle-Blower Hotlines and Anonymous Reporting

There are no official whistle-blower's laws or policies under Egyptian legislation and there is no evidence that the DPL plays a role in setting up whistle-blowing operations. However, the Cybercrimes Law regulates online activities that involve content violations, as it covers offences against confidentiality, integrity of computer data, and invasions of privacy. Hence, the Cybercrimes Law governs a variety of issues related to online crimes that violate sensitive contents.

In light of the above, an employer who empowers employees to speak up without fear of punishment can help the authorities both detect and deter cybercrime violations. Encouraging employees to report wrongdoing and to protect them when they do so, is essential in preventing corruption in both the public and private sectors.

E-discovery Issues

The Protection of Intellectual Property Rights Law No 82 for 2002 (IPL) protects inventions of the human intellect, including creative concepts, inventions, industrial models, trade marks, songs, literature, symbols, names, brands, etc. Generally, employees have the same ownership rights to an invention as other inventors. However, there is an exception to the above, where the IPL states that the employer shall have all the rights derived from the inventions discovered by their employee(s) during the period of their work relationship or employment, as long as the invention was created while the person was still employed, in a work relationship with the employer, or under an employment contract with them. Moreover, the IPR states that the employee who created the invention must be mentioned in the patent and, even if such payment was not agreed upon, must be paid for their work.

2.5 Enforcement and Litigation

Overview

Egypt is a civil law jurisdiction where the law is based on the Napoleonic civil code. Litigations are conducted before the competent public Egyptian courts. The courts system has three levels of litigation: first instance, appeal and cassation. Alternative dispute resolution mechanisms (such as arbitration) are available in civil and commercial disputes pursuant to Arbitration Law No 27 of 1994, as amended (the "Arbitration Law"). Class actions are not generally prohibited under Egyptian law and are sometimes recognised in specific proceedings, such as collective employment disputes and in bankruptcy proceedings. Actions in connection with breach of the DPL would normally be brought before the competent Egyptian court (in this case, the Economic Court).

The telecommunications sector in Egypt is broadly regulated under the Telecommunications Law. Among the key principles adopted under the Telecommunications Law is the customer's right to preserve the secrecy of their information. Telecommunications service providers are therefore required to put in place sufficient measures to preserve and protect customers' information.

The Egyptian Constitution of 2014, as amended (the "Constitution") admitted the right to the privacy and confidentiality of communications (Article 57). Article (99) of the Constitution allows aggravated subjects, due to privacy invasion, to

initiate direct action (without recourse to public prosecution), as follows:

"Any assault on the personal freedoms or sanctity of the life of citizens, along with other general rights and freedoms guaranteed by the Constitution and the law, is a crime with no statute of limitations for both civil and criminal proceedings. The injured party may file a criminal suit directly."

The invasion of privacy is also criminalised under Articles 309 (bis) and 309 bis (A) of the Penal Code, as amended. Establishing the standard of proof and evidence collection in criminal matters is subject to Criminal Procedures Law No 150 of 1950, as amended ("Criminal Procedures Law").

Although privacy and data protection seem at a glance to be synonymous, they are different in a legal context. While data privacy deals with the right to preserve and enable access to information owned by an individual or legal entity, data protection is the right to disallow and enforce protection against unlawful disclosure of personal data. The differentiation is important in understanding the course of action and regulatory procedures applicable.

Due to the increased use of IT in various fields, the need to have special laws to deal with matters of privacy and data protection in digital and tech practices has become unequivocal. This need was notably realised under the DPL and the Cybercrimes Law.

The DPL regulates personal data collection and processing activities. Acts committed in breach of the DPL will be subject to the sanctions set in any of the following cases:

- the person committing the breach is an Egyptian national, whether the act took place inside or outside of Egypt;
- the act was committed by a non-Egyptian residing in Egypt; or
- the act was committed by a non-Egyptian not residing in Egypt, as long as that act is sanctioned in the country where the act took place and the data in question belongs to Egyptians or non-Egyptians residing in Egypt.

By contrast, the DPL scope excludes, inter alia, personal data of third parties which is held by natural persons and processed for personal use, personal data collected, kept or processed in prosecution files, judicial files, national security, official statistics, media and journalism, and the banking sector – except money remittance and exchange companies ("Excluded Activities").

Data protection and privacy infringements are primarily subjected to the DPL and the Cybercrimes Law. There are no particular legal standards currently enacted to report, establish or prove a regulatory violation in connection with the DPL. This is mainly because the DPL refers the relevant procedural steps to the DPL executive regulations, which are yet to be issued. Due to this stance, it is currently difficult to predict the exact standards required to establish alleged violations under the DPL.

The DPL

The main regulatory body mandated to oversee the application of the DPL and to regulate personal data collection and processing activities is the DPC. The DPC is a general economic authority following the Minister of Telecommunications and Information Technology. The decree naming the DPC members and their formation has not yet been issued, making the implementation

and enforcement side of the DPL uncertain in practice.

At the outset, violation of personal data privacy ("Breach of Data Privacy") is defined under the DPL as "unauthorised or unlawful access to personal data or any other unlawful means to copy, send, distribute, exchange, transmit or circulate data which targets the disclosure, dissemination, damage, or amendment of personal data while being stored, transmitted or processed".

The DPL broadly prohibits the collection, processing, disclosure or dissemination of personal data without the express consent of the data subject, or as otherwise permitted by the law. The DPL also sets out the general rights of the data subject in the matter of data protection ("Rights"), which include:

- knowing their personal data is held by the data possessor, the data controller or the data processor;
- previewing, reaching and receiving their personal data;
- withdrawal of preapproval to keep or process their personal data;
- amending, correcting, deleting, adding to or updating their personal data;
- allocating data processing in a particular area (or for a particular purpose);
- to be informed of any breach or violation of their personal data; and
- to object to the data processing or outcome thereof if this contradicts the basic rights and freedoms of the data subject.

In addition to the Rights, the DPL also sets out the procedures to be implemented by the data controller, data possessor and data processor in disclosing personal data, as follows:

- the disclosure must be based on a written request from an authorised subject or based on a legal document;
- all the documents required to make the disclosure must be available; and
- a decision on the request must be made within six days of the date of submission.

The DPC's employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Minister of Telecommunications and Information Technology, who is the competent minister in this regard, have judicial control powers in relation to violations committed under the DPL. Breaching the DPL triggers (i) administrative liability, (ii) civil liability, and (iii) criminal liability (as applicable).

Administrative liability

Under the DPL, carrying out personal data collection, processing or transmission activities requires obtaining the relevant permit or licence from the DPC in accordance with the DPL. The DPL also poses an obligation to the data processor and the data controller to report any violation or dissemination of personal data to the DPC within 72 hours.

Breaching any of the regulatory obligations will trigger administrative measures against the breacher to be imposed by the executive president of the DPC, as follows:

- issuing a warning to suspend the licence, permit or approval for a period of time (whether partially or entirely);
- stopping the licence, permit or approval (whether partially or entirely);
- revoking the licence, permit or approval or cancelling any of these (whether partially or entirely);

- publishing a statement in the media describing the contraventions, at the cost of the breacher; and
- imposing technical supervision from the DPC on the data processor or the data controller (as applicable) at their cost.

The DPL also allows the data subject to administratively exercise and report a breach of data privacy, as follows:

Requests

The data subject, or any authorised third party, may submit a request in connection with exercising their rights to the data possessor, controller or processor. The response to the request should be made within six days of the date of submission of the request.

Complaints

The data subject, and any authorised third party who has a direct interest thereto, may submit a complaint to the DPC in any of the following events:

- violation or breach of the Rights;
- disallowing the data subject to exercise their Rights;
- decisions issued by the DPO in connection with requests submitted to it.

The DPC will look into the complaint and undertake the necessary investigatory procedures. The DPC will then issue its decision within 30 days of the date of submission of the complaint and notify the parties. The defendant must implement the DPC decision within seven business days from the date of notification of the decision and inform the DPC on the steps taken in this respect. The exact means of enforcement and relevant measures thereto will be further established under the DPL executive regulations.

Civil liability

Civil liability would be invoked on the basis of Civil Law No 131 of 1948 (the "Civil Code"). Civil liability would stem either from a breach of contractual obligation (eg, where a contract is in place between the data subject and the data processor/data controller) or tort liability. The rules of evidence in connection with civil matters are further set forth under the civil and commercial Proof Law No 25 of 1968, as amended (the "Evidence Law").

The general principle adopted under the Evidence Law is that who pleads must prove. In civil matters, the evidence would broadly rely on written documents presented by the parties, in addition to other means of proof such as testimony, clues, inference and expertise. The Egyptian courts will reserve the right to decide on the matter based on the evidence submitted by the parties in presenting their case.

On the other hand, in tort liability, the claimant will have to prove the occurrence of damage and establish the link (causality) between the damage and the tortious act. While contractual liability allows the aggravated party to receive a forced execution of the liability in breach under the contract in addition to indemnification (as applicable), the tort liability will give rise only to the right to receive an indemnification against the damage that occurred. The amount of indemnification would generally be determined and ordered by the court.

Criminal liability

The DPL sets out a number of acts which are deemed criminal. Crimes committed under the DPL will be decided by the competent Economic Court (Article 5 of the DPL promulgation provisions).

The DPC's employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Minister of Telecommunications and Information Technology, who is the competent minister in this regard, have judicial control powers to prove crimes have been committed under the DPL.

In addition to the monetary penalty applicable against regulatory violations, a prison sentence (varying from three to six months) would apply in the case of:

- unlawful dissemination of personal data against receiving benefit or exposing the data subject to harm;
- the collection, processing or dissemination of sensitive personal information without the consent of the data subject or the cases permitted by law;
- breaching the cross-border data transmission rules under the DPL; and
- hindering the DPC representatives (who are vested with jurisdictional power) from exercising their enforcement mandate under the DPL.

Although the DPL recognises the evidentiary value of digital proof derived from personal data, the DPL referred the technical conditions required for that digital proof to be established to the DPL executive regulations (not presently issued).

In addition, in crimes resulting from using digital and IT means, criminal liability would be established in accordance with Cybercrime Law No 175 of 2018 (the "Cybercrime Law") and its executive regulations issued by Cabinet Ministers' Decree No 1699 of 2018 (the "Cybercrime Law executive regulations").

There are presently no available enforcement or practical precedents in connection with the DPL, as it is fairly new and the executive regulations are awaited.

Cybercrimes Law

The Cybercrimes Law broadly applies to various forms of criminalised acts that use IT and digital means. The Cybercrimes Law works in conjunction with other legislation, including the DPL and the Telecommunications Law, as amended.

Telecommunications service providers are required to obtain a relevant licence or permit from the NTRA, which is the main regulatory body of information technology services. As with the DPL, breach of the Telecommunications Law or the telecommunications service provider's licence or permit terms and conditions would trigger regulatory action (administrative liability) by the NTRA against the telecommunications service provider concerned, in addition to raising civil liability where the breach resulted in loss or damage.

The Cybercrimes Law criminalises various acts committed by using IT and digital means. These criminal acts are generally categorised as follows:

- encroaching on the security of information networks, systems and technologies;
- infringement of the security of networks, systems and IT;
- crimes committed by using information systems and technology means; and
- crimes relating to the invasion of privacy.

The Cybercrimes Law sets out the obligation of IT service providers to (i) uphold the privacy of user information, and (ii) preserve the secrecy of this information. Criminal liability could be held

against an IT service provider and/or its legal representative where the service provider is a corporate entity.

Moreover, the Cybercrimes Law defines digital proof as follows:

"Any electronic information that has strength or evidentiary value that is stored, transmitted, extracted, or taken from computers or information networks and the like, in the form of magnetic or electrical fields or pulses that can be collected and analysed using special technological devices, programs or applications."

Furthermore, Article (11) of the Cybercrimes Law provides that digital proof can be "obtained or extracted from machines, equipment, intermediary, electronic software, [an] electronic system or computer program or any other information technology which possess material evidential value in criminal matters as long as it adheres to the conditions set forth in the Cybercrimes Law executive regulations".

The procedural steps pertaining to establishing and collecting digital proof and evidence in the matter of cybercrimes are set forth in Article (5) of the Cybercrimes Law. These procedures will be carried out by the appointed NTRA officers (vested with jurisdictional powers) and the investigation body (normally the public prosecutor's office).

The investigation body issues a justified order instructing the NTRA appointed officers, within 30 days (extendable), to conduct any of the following steps:

- to confiscate, collect and track data and information or IT systems, software, programs or computers;
- to search and inspect the data platforms, programs, equipment and other IT systems; and
- to order the service provider to deliver data or information in connection with the information system or equipment under its control, as well as its customers' information and communication trajectory made on this system.

Appeal against these procedural orders would be conducted before the competent criminal court in accordance with the Criminal Procedural Law.

Article (9) of the Cybercrimes Law executive regulations further sets out the standards required to accept digital proof as evidence in the matter of cybercrimes, as follows:

- the process of collecting, acquiring, extracting or deriving the digital evidence in question is carried out using techniques that guarantee not to change, update, erase or distort writing, data and information, information systems and programs, or electronic supports and others (including, in particular, Digital Images Hash, Write Blocker, and other similar technologies);
- that the digital proof provided is relevant to the fact and is within the context of the matter to be proved or denied, in accordance with the scope of the decision of the investigating body or the competent court;
- that the digital proof was collected, extracted and preserved by the judicial control officers authorised to deal with such evidence, or by specialised experts assigned by investigative or trial bodies; on the condition to be indicated in the records of the seizure, or technical reports, of the type and specifications of the programs, tools, devices and equipment that have been used, and that the hash code and algorithm resulting from the extraction of

a similar or identical copy of the original from the digital directory will be documented with the recording or technical inspection report to ensure that the original is preserved without tampering;
- where it is problematic to review the copy of the digital proof and to seize the equipment being verified for any reason, the original will be examined and the foregoing difficulties will be recorded in the seizure or inspection reports; and
- that the digital evidence is documented with a record of procedures by the specialist before the examination and analysis operations take place, as well as documenting the place of the digital proof seizure, preservation, dealing and specifications.

The current penalties imposed on cybercrimes range from a minimum monetary fine of EGP10,000 and a maximum monetary fine of EGP10 million, as well as imprisonment ranging from a minimum of three months to a maximum of five years.

In the matter of the Cybercrimes Law, the court of cassation in case No 15802 of judicial year 90 decided on the scope of application of Article (25) of the Cybercrimes Law. This is in connection with a video depicting assault posted on Facebook. The question was whether this posting constituted a violation of privacy in the sense of Article (25) of the Cybercrimes Law, which states that:

"Anyone who attacks any of the family principles or values in Egyptian society, violates the sanctity of private life, or sends numerous electronic messages extensively to a particular person without his consent, or publishes through the information network or by one of the means of information technology information, news, images and the like that violate the privacy of any person without his consent, whether the information published is true or incorrect, shall be punished by imprisonment for a period of not less than six months, and by a fine of not less than fifty thousand pounds and not exceeding one hundred thousand pounds, or by either of these two penalties."

The court found that the posts on Facebook documented what really happened, according to various police reports filed on the same day of posting on Facebook, and the posts did not include any offensive words to the claimant. The court also did not find any violation of the claimant's private life in what the defendant had posted and thus decided to dismiss the application of Article (25) of the Cybercrimes Law.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Access to data by law enforcement to evidence matters relating to crimes is generally subjected to the Criminal Law and the Criminal Procedural Law. The standard process will require issuing an order from the public prosecutor or the competent court to permit and direct on accessing the data to evidence the criminal act. Crimes are generally subject to the Penal Code. Under the Penal Code, criminal acts are classified into three main categories:

- contraventions, which are crimes punished by monetary fine;
- misdemeanours, which are crimes punished by imprisonment (for a period not exceeding three years) and a monetary fine; and

- felonies, which are crimes punished by imprisonment (for a period over three years), capital punishment, lifetime imprisonment, and aggravated imprisonment.

Acts made in breach of the DPL are subject to a maximum prison sentence of six months and a monetary fine of up to EGP5 million (as applicable). The regulatory standards required to establish breaches of data privacy have not yet been enacted (see **2.5 Enforcement and Litigation**).

Besides the available regulatory routes (such as requests and complaints), the DPL has not set particular procedures to be followed to report a breach of data privacy.

Article (1) of the Criminal Procedures Law provides that the public prosecution is the jurisdictional body mandated to initiate and undertake criminal action and proceedings, except where stated otherwise in the applicable law. In the cases specified under the Criminal Procedures Law, the initiation of criminal proceedings will require submission of a written complaint to the public prosecution or a request to the competent authority (as applicable). Based on the DPL and the Criminal Procedures Law, crimes relating to breaching data protection will not generally fall under the cases required to file a complaint with the public prosecution.

On the other hand, the Cybercrimes Law imprisonment penalty varies between one month and five years (as applicable). The Cybercrimes Law also sets out, in addition to means of establishing digital proof (see **2.5 Enforcement and Litigation**), the available procedures in respect of cybercrimes.

Article (5) of the Cybercrimes Law permits the Minister of Justice to confer jurisdictional powers to the NTRA officers, or other officers nominated by national security authorities, to carry out law enforcement and prove crimes committed under the Cybercrimes Law.

Furthermore, Article (6) of the Cybercrimes Law deals with temporary judicial writs as follows:

"The concerned investigation body, as the case may be, could issue a substantiated writ to the competent law enforcement officer in respect of one or more of the following matters, for a period not exceeding 30 days renewable for one time, if this will help reveal the truth about the perpetration of an offence punishable under this law:

- Control, withdrawal, collection, or seizure of data and information or information systems, or tracking them in any place, system, program, electronic support or computer in which they are existing. Its digital proof shall be delivered to the body issuing the order, provided that it shall not affect the continuity of the system and provision of the service, if so required.
- Searching, inspecting, accessing and signing in the computer programs, databases and other devices and information systems in implementation of the seizure purpose.
- Ordering the telecommunications service provider to submit the data or information related to an information system or a technical device under the control of or stored by the telecommunications service provider, as well as the data of the users of its service and the connection traffic made in that system or the technical system (emphasis added).

In all cases, the writ issued by the investigation entity must be substantiated. The aforesaid writs shall be appealed before the competent criminal court, to be held in the deliberation room on the

dates and according to the procedures stipulated in the Criminal Procedures Law".

Moreover, Article (9) of the Cybercrimes Law permits the general prosecutor, or other concerned investigation authorities, as necessary or where sufficient evidence establishes the seriousness of the crime, to issue a travel ban order against the accused for a defined period of time. The person against whom the travel ban was issued may file a grievance before the criminal court against the travel ban decision within 15 days. If the grievance is rejected, another grievance may be submitted after three months has lapsed from the date when the court rejected the original grievance.

3.2 Laws and Standards for Access to Data for National Security Purposes

National security is protected under the Constitution and supervised by the national security council (NSC) established by way of Presidential Decree No 19 of 2014. Egypt has also promulgated Anti-terrorism Law No 94 of 2015 (the "Anti-terrorism Law"), which is a cornerstone of national security. Furthermore, Egypt is a signatory of a number of international treaties dealing with cybercrimes and judicial collaborations in crimes and national security-related matters (see **3.3 Invoking Foreign Government Obligations**).

Generally, access to data and information by government agencies, to investigate a crime or preserve national security, is not subjected to particular investigation standards or procedures.

At the outset, the Telecommunications Law defines "national security" as follows:

"Matters relating to the presidency, armed forces, ministry of interior, national security authority, administrative control authority and any entity relating to these authorities".

The NTRA mandate includes protecting national security. The NTRA board members include representatives of the ministry of defence and national security authorities. Telecommunications service providers are required to observe national security needs as per the obligations set under the licence.

Article 64 (2) of the Telecommunications Law provides that:

"With due consideration to the inviolability of citizens' private life as protected by law, each telecommunications operator (emphasis added) and service provider shall, at his own expense, provide within the telecommunications networks licensed to him all technical potentials including equipment, systems, software and communication which enable the armed forces and national security entities to exercise their powers within the law. The provision of the service shall synchronise in time with the availability of required technical potentials. Telecommunications service providers and operators and their marketing agents shall have the right to collect accurate information and data concerning users from individuals and various entities within the state."

Also, Article (67) of the Telecommunications Law provides that:

"The state competent authorities shall have the power to subject to their administration all telecommunications services and networks of any operator or service provider and call operation and maintenance employees of such services and networks in case of natural or environmental disasters or during declared periods of general mobilisation in accordance with the provisions of

Law No 87 of 1960 or any other cases concerning national security."

Meanwhile, the Cybercrimes Law upholds a broader definition of national security, as follows:

"Means anything relating to the independence, stability and safeguard of homeland, preserving its unity and territorial integrity, and matters relating to presidential affairs, the NSC, national defence council, ministry of defence, ministry of the interior, general intelligence, administrative control authority and entities affiliated thereto."

A particular caveat was added in Article 2 (3) of the Cybercrimes Law which provides that:

"With due regard to the sanctity of private life, telecommunications service providers (emphasis added) and their affiliates are under an obligation to provide national security entities, in accordance with their needs, all technical means to enable these entities to exercise their mandate in accordance with the law."

By contrast, the Anti-terrorism Law provides exceptional procedures in the matter of accessing data and information to investigate crimes relating to terrorism. For instance, Article (46) of the Anti-terrorism Law provides that the general prosecution or other investigation authorities may, in investigating a terrorist crime, issue an order (valid for 30 days) to tape, monitor and record conversations and messages carried by way of wireless or wired communications or other technology means, including those communications made in private places.

3.3 Invoking Foreign Government Obligations

Generally speaking, it is not permissible for an organisation to invoke a foreign government's access request to collect or transfer personal data, except where the law permits this or there is an international treaty between the Egyptian government and the foreign government, permitting the latter to collect and transfer personal data on a legitimate basis. In this regard, Egypt is a party to several bilateral and multilateral treaties where it is agreed that information, evidence, records, etc will be shared between the parties. These treaties include the following.

- The Treaty Between the Government of the United States of America and the Government of the Arab Republic of Egypt on Mutual Legal Assistance in Criminal Matters, signed in 1998, where the scope of assistance between the contracting parties is specified under Article (1), stating that "The contracting parties shall provide mutual assistance, in accordance with the provisions of this treaty, in connection with the investigation, prosecution, and prevention of offences, and in proceedings relating to criminal matters." Although the treaty did not specifically mention that mutual assistance is specifically related to personal data and privacy, the means of assistance listed under Article (1) (2) could entail the provision of personal information, as it is stated that assistance shall include "…(b) providing documents, records, and items of evidence; (c) locating or identifying persons or items; (d) serving documents… (h) any other form of assistance not prohibited by the laws of the Requested State [emphasis added]".
- The Arab Convention on Combating Information Technology Offences, entered into force in Egypt by the issuance of Presidential Decree No 276 for 2014, where the Fourth Chapter regulates the legal and judicial assistance between the parties. In particular, Articles 38, 39, 40, 41, 42 clarify the scope

of assistance in relation to (a) the expeditious disclosure of safeguarded users' tracking information, (b) the access to stored information, (c) the access to IT across borders, (d) the expeditious gathering of users' tracking information, and (e) the assistance regarding information related to content.

- The Foreign Account Tax Compliance Act (FATCA) enacted in 2010, which aims at curbing tax evasion by US citizens and residents through the use of offshore accounts operating outside the US. Foreign financial institutions in Egypt are required to enter into disclosure compliance agreements with the US Treasury and report information regarding financial accounts held by US taxpayers, or held by foreign entities in which US taxpayers hold a substantial ownership interest. In practice, banks would conclude relevant FATCA agreements with concerned clients to enable the enactment of reporting.
- The United Nations Convention Against Corruption (UNAC), entered into force in Egypt on 2005, where Article (46) states that mutual legal assistance may be requested for the purpose of "…(e) providing information, evidentiary items and expert evaluations; (f) providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records… (i) any other type of assistance…"
- The 1988 Vienna Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, entered into force in Egypt in 1991, where Article (7)(2) states that mutual legal assistance may be requested for the purpose of "…(f) providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records…" and where Article (7)(5) states that, "A party shall not decline to render mutual legal assistance under this article on the ground of bank secrecy."
- The United Nations Transnational Organised Crime (UNTOC) agreement, entered into force in Egypt in 2004, where Article (18) states that mutual legal assistance may be requested for the same purposes stated in the 1988 Vienna Convention.
- The International Convention for the Suppression of the Financing of Terrorism, entered into force in Egypt in 2005, where Articles 12, 13 and 14 state that parties shall afford one another the greatest measure of assistance concerning evidence required for criminal investigations or extradition proceedings regarding acts of financing terrorism.

Egypt has not, however, so far participated in a Cloud Act agreement with the USA.

In addition to the above, Anti-money Laundering Law No 80 of 2002 (the "Anti-money Laundering Law") grants the Anti-money Laundering and Terrorist Financing Unit, (the "Unit") the authority to receive notifications from financial institutions and non-financial professions and businesses about transactions suspected of involving money laundering or terrorist financing, or attempts to carry out such operations. The Unit, in response, may create a database of the information available to it, where it may exchange this information with the competent authorities in foreign countries and international organisations, in application of the provisions of international agreements to which Egypt is a party, or in application of the principle of reciprocity.

3.4 Key Privacy Issues, Conflicts and Public Debates

Due to the newness of the DPL, it is not considered to be executed in practice in Egyptian soci-

ety to date. Therefore, it has been publicly noted that the DPL still needs to cope with the ongoing worldwide developments in the data privacy and protection fields. For this reason, it is difficult to address significant issues in this regard until the DPL and its awaited executive regulations apply to all individuals and entities in practice.

4. International Considerations

4.1 Restrictions on International Data Issues

The DPL introduces restrictions and controls on the cross-border or international transfer of data as a means to protect the subject whose data is being transferred (see also **3.3 Invoking Foreign Government Obligations**).

Articles 14–16 of the DPL are concerned with said cross-border transfer of data. The main restriction stated by the law is ensuring that the level of protection of data implemented in the state to which the data is being transferred is the same or exceeds the level of protection required in Egypt. The level of protection of the foreign state will be examined by the DPC, which will be established pursuant to Articles 19-25 of the DPL. Consequently, if the level of protection is found adequate and conforms with that of the DPL, a licence or permit will be granted by the DPC in order to be able to transfer the data.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

As a general rule, no derogations apply to international data transfers except under the approval of the data subject. Nevertheless, the DPL states that this is permissible as an exception, in the case of the express consent of the person whose data it is, or their representative, to transfer, share, trade or process personal data with a country that does not have the level of protection referred to in **4.1 Restrictions on International Data Issues**, in the following cases:

- to preserve the life of the person whose data it is, providing medical care or treatment, or managing health services for them;
- to execute obligations to ensure proof of right, exercising or defending this before the judicial authorities;
- to conclude a contract, or the execution of a contract already concluded, or to be concluded, between the person responsible for the processing and a third party, for the benefit of the person whose data it is;
- to implement a procedure for international judicial co-operation;
- due to the existence of a legal necessity or obligation to protect the public interest;
- to make cash transfers to another country in accordance with its specific and applicable legislation; and
- where the transfer or circulation takes place in implementation of a bilateral or multilateral international agreement to which the Arab Republic of Egypt is a party (see **3.3 Invoking Foreign Government Obligations**).

In addition, criminal investigation could act as an exception to the transfer of international data, as elaborated in **2.5 Enforcement and Litigation**. Finally, international data transfers may also be enacted where Egypt's national security requires this, in accordance with the need to enable these entities to exercise their mandate in accordance with the law, as designated under **3.2 Laws and Standards for Access to Data for National Security Purposes**.

4.3 Government Notifications and Approvals

As explained in **4.1 Restrictions on International Data Issues**, the DPC's approval is required in order to obtain a licence or permit to proceed with transferring data across the border. The DPC has to be notified prior to the transfer of said data. Chapters 9 and 10 of the DPL discuss the role of the DPC when it comes to granting approvals and the required licences and permits, and the procedures required.

In order to apply for said licence or permit, an application must be submitted on the forms produced by the DPC attaching all the necessary supporting materials, demonstrating the applicant's financial stability and the applicant's technical competence. Following the completion of all the applications, decisions must be made within a timeframe of no more than 90 days. The application will be declared rejected if the allotted time has passed without a decision from the relevant authority in the DPC.

In deciding whether to approve or reject the application, the DPC may ask for further information, papers or documents. In the event that the protection stated in the supplied papers is insufficient, the DPC also has the right to seek the provision of additional guarantees for the protection of personal data.

It is worth mentioning that the DPC, in accordance with public interests, may amend or change the provided licences or permits, even following their issuance, if:

- new or relevant international, regional and/or local regulations have been issued which affect cross-border matters;
- the licensee has requested to amend the purpose of their licence;
- the data controller or data processor is going to merge with other entities or persons outside Egypt; and
- amendments are deemed necessary in order to continue implementing the rules of the DPL.

4.4 Data Localisation Requirements

The DPL stresses the fact that data should remain within the borders of Egypt. By doing so, it ensures the protection of any type of data for the protection of the public interest. The DPL mentions the establishment of the DPC, which will be responsible for localising the data. In addition to the DPC, other data localisation centres are already established and are adhering to the rules of the Telecommunications Law until the executive regulations of the DPL are issued.

Said data centres require specific licences in order to be registered and able to operate, and these licences can be obtained from the NTRA. These centres can be differentiated by whether they will operate within or outside Egyptian borders.

- Private data centres: these are established by a natural or legal person for their own exclusive use, without making the centre available in whole or in part to any other party. No specific registration or licences are required whether operating inside or outside Egyptian borders.
- Co-location/multi-tenants' public data centre provider (PDCP): these data centres are established within Egypt for the purpose of hosting service providers. No specific registration or licences are required when operating outside of Egypt; however, a licence is required when operating inside Egypt.
- Cloud service provider (CSP): these are companies providing cloud services of all kinds,

whether through wholly owned data centres or leased from licensed PDCPs. No specific registration or licences are required when operating outside Egypt; however, registration as a CSP is required when operating inside Egypt.

4.5 Sharing Technical Details

Egyptian laws and regulations do not state that any specific software codes, algorithms, or any similar technical details should be shared with the government.

4.6 Limitations and Considerations

As stated in **4.2 Mechanisms or Derogations That Apply to International Data Transfers**, the DPL considers government requests and litigation proceedings to be an exception to the requirement of level of protection. It is worth mentioning that the DPL is inspired by the GDPR.

4.7 "Blocking" Statutes

Prior to the issuance of Press and Media Regulations Law No 180 of 2018 (the "Media Law"), the Constitution prohibited imposing censorship over Egyptian newspapers and media outlets, or confiscating, suspending or closing them, as there were no legal provisions regulating the process of blocking and filtering content of different forms. As a result, the administrative court used to apply the Telecommunications Law provisions as a legal buttress, or perhaps as an excuse for blocking newspapers and media outlets. It can be said that such judicial jurisprudence has contributed to establishing legal rules to allow "blocking" of various media content.

Accordingly, post the issuance of the Media Law, a number of rules now regulate the operation of media outlets of various forms. In this regard, the Media Law vests the Supreme Council for Media Regulation (SCMR) with vast competencies allowing it to impose different forms of censorship over the different forms of media outlets. The Media Law further widened the scope of competence of the SCMR, as a result of which, distinctions between different forms of censorship and their mechanics all fall under the discretion of the SCMR.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The DPL has great interest in the collection of data, big data, AI, and the IoT, due to Egypt's dependence on these advanced technologies.

The mechanism of AI requires the collection of big data and learning the patterns of those data. In other words, a large set of data is combined for a specific task or mission through an intelligent collection process, where several patterns are found in the collected data. As a result, outcomes can easily be predicted for specific outputs.

In light of the above, any collected and/or processed data for the purpose of AI technology, is protected under Egyptian law. In this regard, the General Conditions (referred to in **1.1 Laws**) must be met.

Similarly, IoT technology mainly depends on the collection of data and its exchange, analysis and processing. Therefore, an IoT service provider is obliged to take all the necessary institutional and technical procedures and steps to protect the confidentiality of the information and data of the service users, as per the general obligations prescribed by the NTRA IoT regulatory framework. Furthermore, it is explicitly stated under the same framework that it is subject to the pro-

visions of the Telecommunications Law and, in particular, the Data Protection Law in this regard.

Apart from the above, contemporary and advanced technologies are not yet specifically addressed under Egyptian law; however, the general rules of law apply.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Currently, there are no digital governance or fair practice review boards enacted under Egyptian legislation. It is worth noting that most regulated activities, such as fintech, financial markets, banking and technology, are generally required to observe certain regulatory requirements under the provisions of the respective applicable laws. For instance, the NTRA established the Consumers' Rights Protection Committee (CRPC) in August 2004, which tries to make all users of the telecommunications sector more aware of their rights by launching campaigns that are mainly related to consumer rights. These rights include the right to "have the confidentiality of [their] data and information protected" and "to resort to the operator's customer service in case [the consumer] has a query or complaint that should be addressed and resolved".

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

See **2.5 Enforcement and Litigation** and **3. Law Enforcement and National Security Access and Surveillance**.

5.4 Due Diligence

There are no specific due diligence requirements in connection with data protection under the applicable laws in Egypt. However, regulated activities especially in telecommunications, banking, and non-banking finance fields are subject to lengthy regulatory and reporting requirements, including those relating to data protection. In this sense, proper due diligence should closely review the activity of the entity concerned and assess the obligations and compliance levels required under the applicable law. In addition, it is important to verify all corporate and regulatory requirements, internal governance, reporting, and procedures in connection with data protection to anticipate the possible risks associated with a breach of privacy or data protection rights.

5.5 Public Disclosure

Capital Markets Law No 95 of 1992 mandates disclosure in several respects; for instance, Article 85 (bis) obliges each company subscribed to the Egyptian Stock Exchange to include a summary of disclosures in its prospectus relating to: (a) the nature of the company's business, and (b) the process of proposition.

In addition, Article 135 (9) obliges companies that work in the field of financial securities to include, with their license request, the company's internal regulations, prohibiting the use of information available to such companies through the process of categorisation.

Article 263 further gives brokerage companies the choice to receive client orders by telephone, in accordance with a telephone system prepared by the company and approved by the FRA, in order to ensure that there is no manipulation or cheating, provided that the client accepts such process in writing.

Finally, Section 7 states that a company that operates in bond brokerage activities must disclose in writing to its clients the specific details of each transaction before its execution. In addition, it must notify the FRA on a daily basis of

the total market value of the bonds it holds, in accordance with FRA regulations.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws

See **2.2 Sectoral and Special Issues**. The DPL is generally based on and reflects the GDPR of the EU. Data protection, as a concept, is still novel and the precedents in connection with enforcement are not currently available.

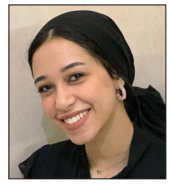
5.7 Other Significant Issues

It is important to note that Egypt's data protection and privacy landscape still requires many upgrades and enhancements to streamline legal and regulatory applications. Due to its recent introduction, the DPL is still not yet tested in practice and is still new to Egyptian society. Furthermore, the DPL will need to cope with ongoing worldwide developments in the data privacy and protection fields, and more awareness needs to be raised in this respect.

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

Authors

Nevine El-Shafei joined Shehata & Partners as a partner in 2022 and has 15 years' experience in both inhouse and private practices in Egypt, Qatar and across the MENA Region. Her practice at S&P focuses on corporate, commercial, TMT and pre-contentious matters. Nevine has extensive experience in the banking and finance sectors and has advised on a broad range of complex transactional and cross-border files. She also has substantial experience in the telecommunications and real estate fields. Nevine has a masters in law from Université Paris 1 Panthéon-Sorbonne, France, and a masters in business international law from Paris Dauphine in France and Cairo University. She also has a diploma in International Commercial Arbitration from the Chartered Institute of Arbitrators in the UK.



Tasneem El-Naggar is an associate with more than two years' experience in the corporate department. She recently joined Shehata & Partners, having started her career at Khodeir & Partners and having interned at several top-tier law firms in Egypt. She has been able to assist a number of Egyptian start-ups, such as Seqoon, The Food Lab and Balad, to do business smoothly and efficiently in Egypt. Tasneem has also been actively involved in the automotive sector, assisting Yazaki to develop its private free zone project in Egypt. In addition to delivering strategic advice to Balad, she has also actively advised other up-and-coming starter businesses in the fintech sector.

Dina El-Saiedi recently joined Shehata & Partners, having previously been involved with several key start-up accounts in Egypt, advising them on how to adopt a business mindset. In addition to interning in several top-tier law firms in Egypt, she has also invested her time in learning how different aspects of the legal and business fields intertwine. Dina has proved to be an integral member of Shehata & Partners, having a keen eye for developments within the Egyptian legal field.

Shehata & Partners

Cairo Business Plaza
North Tower
2nd Floor, Unit (204)
New Cairo
Cairo
Egypt

Tel: +2 28135682
Email: info@shehatalaw.com
Web: shehatalaw.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com