EGYPT

Law and Practice

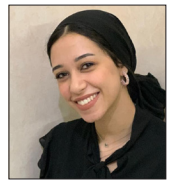
Contributed by:
Ibrahim Shehata, Tasneem El-Naggar and Safa Rabea
Shehata & Partners

Contents

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

Authors

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



Tasneem El-Naggar is a mid-level associate at Shehata & Partners, with expertise in corporate law, commercial transactions and regulatory compliance. She interned at several top-tier Egyptian law firms before beginning her career in arbitration at Khodeir & Partners. She holds a diploma in Public Law from Ain Shams University and is currently pursuing her master's degree. Tasneem has advised on major projects, including Yazaki's private free-zone establishment in Egypt, and has supported emerging fintech ventures. Her experience spans diverse fields, from drafting contracts for theatrical productions in Saudi Arabia to advising AI-driven start-ups, demonstrating her adaptability across industries.

Safa Rabea recently joined Shehata & Partners as a junior associate, specialising in corporate governance and commercial law. She previously completed internships at top-tier law firms, gaining valuable experience in banking and finance, arbitration and M&A transactions. Safa then joined Al-Hussien and Partners, where she advised on corporate transactions, compliance and risk management, further strengthening her legal expertise.

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

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

A Framework for Safeguarding Personal Information

Data privacy has emerged as a paramount concern for both individuals and businesses globally. Recognising the critical importance of safeguarding personal information, especially in the emergence of the digital age, Egypt has established a comprehensive data protection framework to address the growing challenges posed by the increasing digitisation of society and the heightened risk of cyber threats.

In light of the above, Egypt issued Personal Data Protection Law No 151/2020 (PDPL) in 2020, which encompasses the protection of individuals' and entities' data and privacy rights. The PDPL generally prohibits the processing of personal data without the explicit consent of data subjects, and grants them multiple rights in restricting access to their data, withdrawing their prior consent and being informed of any data violation.

Under the PDPL, any digitally collected and/or processed data must meet the following 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.

Constitutional and Legislative Foundations

Generally, the right to privacy is at the heart of the freedom rights established under the Egyptian constitution; the 2014 Egyptian Constitution provides for the protection of individual privacy. The key rights include the following.

- Inviolability of private life: Article 57 of the Constitution states that "Private life is inviolable, safeguarded and may not be infringed upon". This broad provision protects a wide range of personal interests, including:
  (a) protection from unlawful searches, seizures and other forms of bodily harm;
  (b) protection from unlawful entry, search and seizure;
  (c) protection of letters, emails, phone calls and other forms of communication;
  (d) protection from interference with family relationships; and
  (e) protection from the unauthorised collection, use and disclosure of personal data.
- Protection of communications: Article 57 of the Constitution specifically states that "Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable…". This provision further emphasises the fundamental right for all kinds of communication channels to be protected.

The Telecommunications Law

In addition, several laws recognise the right to privacy, such as the Telecommunications Law No 10/2003. Sensitive and emerging technologies, such as AI and IoT, are advanced technologies that include multi-layered interactions and services that require the collection of enor-

mous amounts of personal data. Such advanced technologies are generally subject to the PDPL, which provides a comprehensive framework for protecting personal data.

However, the Telecommunications Law adds an additional layer of protection specific to the telecommunications sector. For example, the Telecommunications Law requires licensed operators to ensure the confidentiality of the communications and private calls of their customers, and mandates the establishment of necessary rules to guarantee this confidentiality, further reinforcing privacy protections in this sector. This sector-specific law reinforces the privacy protections already granted under the PDPL, ensuring robust safeguards tailored to the unique risks posed by telecommunications and emerging technologies.

The Cybercrimes Law

The Cybercrimes Law No 175/2018 on combatting IT crimes and its executive regulation No 1699/2020 regulate online activities and aim to penalise, inter alia, unlicensed online activity and content violations, such as illegally accessing a private device or account, which is a very possible crime under sensitive digital technologies.

Under the Cybercrimes Law, service providers 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.

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 the obtaining and disclosing of personal information without lawful means.
- Law No 15/2004 regulating e-signatures and establishing the Information Technology Industry Development Agency (ITIDA) and its executive regulations provides that applicants for e-signature services must ensure, among other things, a secured system to preserve the secrecy and privacy of the information as per legal standards, and 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 the penalties to be applied when telecommunications service providers breach regulations

by the National Telecommunications Regulatory Authority (NTRA) issued in connection with users' rights protection. These same regulations also 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) obliges 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) obliges 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.

Interplay Between the Egyptian Privacy and Data Protection Legal Framework and the GDPR

The main intention of the authorities issuing the PDPL is twofold: to keep pace with current developments in the field of communications technology and to protect the right to privacy. Most importantly, the PDPL reflects significant influence from the European General Data Protection Regulation (GDPR), incorporating many of its key principles, including the following.

Definitions for data protection

The PDPL outlines a list of definitions for data protection that are binding and are included in the legal framework. According to this principle, the law must contain clear concepts for personal data and sensitive personal data, and must 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 PDPL 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 non-compliance with the data owner's right to view their data.

Legal basis for processing

The PDPL 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 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 PDPL guarantees "the right to withdraw prior consent to the retention or processing of personal data".

Binding users' rights

The PDPL 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 or correction, the right to receive information, and the right to enquire. The PDPL 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, with the Data Protection Centre being responsible for issuing decisions related

to determining and receiving financial compensation.

Clear scope of application

The PDPL outlines a clear scope of application, clarifying in Article (2) that it applies to anyone who commits one of the specified crimes under the PDPL and who is:

- an Egyptian, whether present in Egypt or residing abroad;
- a non-Egyptian residing inside Egypt; or
- 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.

Mechanisms for the secure transfer of data to other countries

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

Considering the above, it appears that the PDPL greatly relates to the multinational principles of the GDPR; however, the PDPL has several shortcomings represented by the failure to involve various groups in society in drafting and preparing the law. It is still possible to address these shortcomings with the issuance of the PDPL executive regulations, through which the authorities can protect and promote privacy and data protection rights.

1.2 Regulators

Key Regulators and Their Respective Areas of Jurisdiction

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

- 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 and approvals, and implementing various measures related to the protection of personal data;
- receiving complaints related to the application of the PDPL to issue the necessary decisions in this regard;
- monitoring those addressed by the PDPL and taking the necessary legal measures;
- checking the conditions for cross-border data movement;
- concluding agreements and memorandums of understanding, and co-operating and exchanging experiences with the relevant international bodies; and
- preparing an annual report on the status of personal data protection in Egypt.

PDPC Judicial Authority

The 13th and 14th chapters of the PDPL grant the status of judicial officers to the employees of the PDPC and prescribe penalties for violating

the provisions of the PDPL, in addition to regulating the methods of reconciliation when any of these violations are committed.

For instance, a fine of no less than EGP100,000 and no more than 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 of between EGP500,000 and EGP5 million where violating the provisions of permits or licences should be pursued under the DPL.

It is worth mentioning that the PDPL has adopted a relatively new punitive act that 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 the breach of their duties can be contributed to the occurrence.

1.3 Enforcement Proceedings and Fines

Administration and Enforcement Process

Practically speaking, there are still no precedents in relation to the administrative process that the PDPC must follow to investigate and impose penalties on PDPL violators, due to the fact that the PDPC has not yet been established, along with the absence of PDPL executive regulations that should regulate such administrative process. Nonetheless, the PDPL states that any person concerned about personal data, who has capacity and direct interest, has the right to complain to the PDPC in the following cases, without prejudice to the right to resort to the judiciary:

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

The complaint will be submitted to the PDPC, which will follow the necessary investigation procedures. The PDPC 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 PDPC's decision within seven working days from the date of notification, and to inform the PDPC of what has been done towards the implementation of its decision.

Calculation of Administrative Fines

The calculation of administrative fines for the violation of data protection is governed by the PDPL, which outlines specific penalties for various offences related to personal data handling, in which it includes both administrative and criminal liabilities. The calculation of administrative fines under the PDPL can vary significantly based on the nature of the offence, with the following examples.

For unauthorised data handling

Any holder, controller or processor who collects, processes, discloses, provides access to or circulates electronically processed personal data without legal authorisation or the consent of the data subject is subject to a fine ranging from EGP100,000 to EGP1 million.

For harmful intent or material benefit
If the violation is committed in exchange for a material or moral benefit, or with the intent to harm or endanger the data subject, the penalty escalates to imprisonment of no less than six months or a fine ranging from EGP200,000 to EGP2 million, or both.

For hindering the rights of data subjects
Any holder, controller or processor who, without lawful justification, denies a data subject their rights under the PDPL shall face a fine ranging from EGP100,000 to EGP1 million.

For cross-border data transfers
Any individual who violates the provisions governing the transfer of personal data across borders is subject to imprisonment for a minimum of three months or a fine ranging from EGP500,000 to EGP5 million, or both.

For sensitive personal data handling
Any holder, controller or processor who collects, processes, circulates, discloses, stores, transfers or saves sensitive personal data without the consent of the data subject or outside the legally authorised circumstances will face imprisonment for a minimum of three months or a fine ranging from EGP500,000 to EGP5 million, or both.

For violation of licences, permits or certifications
A fine ranging from EGP500,000 to EGP5 million will be imposed on any individual who breaches the provisions regarding licences, permits or certifications under the PDPL.

These provisions are designed to ensure strict compliance with the PDPL. The penalties scale with the gravity of the violation, particularly when sensitive data or cross-border transfers are involved, reflecting the heightened risks to individuals' privacy and security.

1.4 Data Protection Fines in Practice

There have been no recent data protection administrative proceedings, as the PDPC has not yet been established and the PDPL Executive Regulations have not yet been issued.

Since the PDPC is designated as the primary data protection regulator in Egypt, its establishment is a prerequisite for the enforcement of activities. However, it is anticipated that the PDPL Executive Regulations will soon be issued.

1.5 AI Regulation

Implications for Data Protection

Recent developments in AI regulation
Egypt has made significant progress in recent years to regulate AI. The National Council for Artificial Intelligence (NCAI), established under Cabinet Decree No 2889/2019, plays a pivotal role in managing the Egyptian AI strategy, focusing on innovation, research and socio-economic development. In addition, the Egyptian Charter for Responsible AI, issued in 2023, serves as a framework for ethical and responsible AI practices, aligning Egypt with global standards such as those of UNESCO and the OECD.

Implications for data protection in the context of AI systems
AI systems rely heavily on the collection and processing of personal data. Egyptian law addresses this through safeguards under the PDPL, including:

- legitimate purpose – personal data must be collected for legitimate, specific and declared purposes;

- accuracy and security – data must be true, sound and secure during collection and processing;
- lawful processing – data must be handled appropriately and lawfully for the stated purposes; and
- retention limitations – data must not be retained longer than necessary to fulfil its purpose.

These safeguards protect personal data used in AI, ensuring compliance with data protection principles.

In addition to the PDPL, the IoT Regulatory Framework issued by the NTRA requires service providers to implement institutional and technical measures to protect user data confidentiality. These provisions extend to IoT systems, which often work alongside AI, ensuring the secure handling of data across interconnected systems.

In addition, the Consumer Protection Law No 181/2018 complements these obligations by requiring service providers to:

- preserve and protect consumer information and data, ensuring it is not disclosed or traded without explicit consent; and
- maintain confidentiality, taking all necessary precautions to uphold the privacy and confidentiality of consumer data.

These combined legal frameworks – the NTRA IoT Regulatory Framework, the PDPL and the Consumer Protection Law – demonstrate Egypt's commitment to safeguarding personal data and consumer rights in the rapidly evolving landscape of technology. Together, they ensure robust protections for personal data while fostering trust in advanced technologies.

Ethical and responsible use of AI

The Egyptian Charter for Responsible AI underscores the principles of transparency, fairness and accountability in AI development and deployment. It provides actionable insights to guide ethical AI practices while aligning with international frameworks, attracting investors and fostering responsible innovation.

Anticipated developments and remaining gaps

While Egypt has made significant strides in regulating AI, specific laws and executive regulations for AI remain absent, with existing legal frameworks, such as the PDPL and Consumer Protection Law, applying general rules to AI-related activities. The issuance of executive regulations and AI-specific legislation is expected to fill these gaps, providing more clarity and robust governance.

Through recent developments such as the establishment of the NCAI and the introduction of the Egyptian Charter for Responsible AI, Egypt has demonstrated its commitment to fostering ethical and responsible AI. These measures position the country as an emerging hub for AI innovation while ensuring the protection of personal data in compliance with legal and ethical standards.

1.6 Interplay Between AI and Data Protection Regulations

Since no official AI-specific regulations have been issued by the NCAI in Egypt, the regulatory framework for AI relies on broader ethical guidelines and existing laws. The Egyptian Charter for Responsible AI, published in 2023 by the Ministry of Communications and Information Technology, serves as the first attempt to articulate ethical and responsible AI practices. This charter adapts international guidelines to the local context, offering preliminary guidance

on the development, deployment and management of AI systems.

Although there are no formal AI regulations, the PDPL indirectly governs AI by imposing safeguards for the collection, processing and retention of personal data. This creates an implicit interplay between data protection laws and the use of AI, ensuring that AI systems comply with existing privacy and security standards.

The Egyptian Charter, while non-binding, reflects the government's commitment to fostering responsible AI use. It positions Egypt to align with global standards and lays the groundwork for future regulatory developments to address specific challenges related to AI.

2. Privacy Litigation

2.1 General Overview

Recent Trends in Privacy Litigation in Egypt

Privacy litigation in Egypt remains in its early stages due to the relatively recent enactment of the PDPL. While enforcement mechanisms are still developing, a clear trend is emerging in cases where individuals' personal data has been violated or misused through communication devices, reflecting the judiciary's focus on safeguarding privacy rights.

Case example: dissemination of private information

In Case No 19754 of 93 Judicial Year, dated 10 September 2024, the appellant was convicted of violating a victim's privacy by disseminating private information and intentionally disturbing her by using communication devices. She challenged the judgment, citing insufficient reasoning, misinterpretation of evidence and a violation of her right to defence. The appellant argued that the judgment lacked clarity and failed to outline the crimes and evidence adequately, and should have been dismissed due to the plaintiff's lack of standing. She also contended that her actions constituted permissible criticism and claimed the court ignored findings from an administrative investigation.

The Court of Cassation rejected the appellant's claims, affirming that the judgment was legally sound, detailed and adequately reasoned. It upheld the conviction, dismissed objections to the admissibility of the case, and ruled that the evidence supported the findings. The court also dismissed the appeal and ordered the forfeiture of the appellant's bail, emphasising the importance of privacy rights and the clarity of judicial reasoning in such cases.

Significance of the case

This case illustrates important aspects of Egypt's emerging privacy litigation landscape, including:

- the recognition of privacy violations – the court's handling of this case highlights the growing seriousness with which privacy breaches involving personal information dissemination are being addressed; and
- judicial clarity and accountability – the Court of Cassation reinforced the need for clear, detailed reasoning in judgments related to privacy violations, ensuring accountability for misuse of personal data.

Privacy litigation in Egypt is gradually evolving, with courts increasingly addressing violations of personal data. Recent cases exemplify the judiciary's commitment to protecting privacy rights, ensuring accountability for privacy violations, and upholding procedural fairness in such cases.

Expected Impact of International Developments on Domestic Litigation

Adoption of global privacy standards

International frameworks such as the EU GDPR are expected to heavily influence domestic privacy litigation in Egypt. The PDPL incorporates many principles from the GDPR, such as transparency, accountability, data minimisation and purpose limitation, and serves as a foundation for privacy protection in Egypt. Courts are likely to refer to the GDPR as a benchmark when interpreting domestic laws, especially in cases involving cross-border data handling or advanced technologies.

Influence on AI and emerging technologies

Global discussions on responsible AI and data protection, led by organisations like UNESCO and the OECD, are expected to shape litigation involving advanced technologies in Egypt. The Egyptian Charter for Responsible AI, which incorporates insights from international standards, may guide court decisions on privacy disputes related to AI.

Increase in cross-border data disputes

As Egypt integrates further into the global digital economy, litigation involving cross-border data transfers is expected to increase. International treaties and bilateral agreements will likely play a significant role in shaping court judgments in cases involving multinational corporations or foreign entities.

Rising consumer expectations

Exposure to international privacy standards such as the GDPR is expected to raise consumer awareness of privacy rights. This heightened awareness will likely lead to increased litigation, with individuals demanding stricter compliance with domestic privacy laws.

Focus on compliance for multinational corporations

International developments may place pressure on multinational corporations operating in Egypt to adhere to higher data protection standards. This is expected to result in more litigation around compliance failures, especially where domestic practices conflict with global obligations.

2.2 Recent Case Law

Key Recent Litigation in Egypt

Recent privacy litigation in Egypt highlights the complexities of balancing national security concerns with data protection rights under the PDPL. A notable case involves the Egyptian Ministry of Interior's objections and appeals concerning the deletion of a defendant's criminal record, showcasing the judiciary's approach to procedural correctness and government accountability.

Case overview

The case revolves around the Egyptian Ministry of Interior filing multiple objections and appeals related to the deletion of a defendant's name from the Ministry's criminal records system. The original ruling, issued by the Administrative Court on 10 April 2021 in Case No 22586 of 74 Judicial Year, required the Ministry to delete the defendant's criminal record after a prior acquittal.

The Ministry argued that retaining the record was essential for national security purposes and invoked Article 5 of the PDPL, which exempts personal data held by national security entities from the law's provisions. Subsequently, the Ministry filed an execution objection in Case No 50804 of 75 Judicial Year on 23 October 2021, seeking to suspend the enforcement of the original ruling.

Judicial rulings

Administrative Court Judgment (23 October 2021, Case No 50804 of 75 Judicial Year):

- the Administrative Court reviewed the Ministry's objection and ruled that execution objections must be based on new facts arising after the judgment, rather than re-arguing the original case;
- it rejected the objection due to the absence of new facts and upheld the enforceability of the original ruling; and
- the court reaffirmed that filing an appeal does not automatically suspend judgment execution unless explicitly ordered by the Appeal Examination Division.

Supreme Administrative Court Appeal (Case No 60817 of 67 Judicial Year):

- the Ministry appealed the Administrative Court's decision but did not obtain a suspension of execution;
- the Supreme Administrative Court ruled that the objection lacked a valid legal basis and rejected it; and
- the Court ordered the Ministry to bear the costs of the proceedings under Article 184 of the Procedures Law.

Legal implications

Article 5 of the PDPL and national security

While the Ministry invoked the national security exemption under Article 5 of the PDPL, neither the Administrative Court nor the Supreme Administrative Court engaged with the merits of this claim. Instead, the rulings focused on procedural issues, highlighting the importance of presenting new facts in execution objections.

Judicial enforcement principles

Both judgments underscore that court rulings must be respected and executed unless a valid legal basis for suspension is provided. This reinforces the rule of law and the finality of judicial decisions.

Accountability in litigation

By ordering the Ministry to bear the costs, the courts sent a clear message about the consequences of raising procedurally invalid objections.

This litigation demonstrates the procedural and substantive complexities of balancing national security concerns with data protection rights under the PDPL. It highlights the courts' emphasis on procedural correctness and the rule of law in disputes involving data protection and government accountability.

2.3 Collective Redress Mechanisms

Egyptian law does not include a dedicated legal framework or specific legislation for collective redress, such as class action lawsuits, as seen in some other jurisdictions, like the EU with the Representative Actions Directive. However, there are procedural avenues through which individuals with similar claims can collectively seek redress, including in cases involving violations of personal data, as follows.

- Representation by associations or legal entities – organisations such as consumer protection associations, labour unions or NGOs can represent groups of individuals in disputes. For example, employees whose personal data has been mishandled by an employer or a labour entity can collectively seek redress with the support of a union. Similarly, NGOs advocating for data privacy rights can assist individuals in pursuing

claims related to data breaches or misuse by companies.
- Consumer Protection Authority – under the Consumer Protection Law, the Consumer Protection Authority is empowered to file lawsuits on behalf of consumers harmed by widespread violations, including cases of unlawful data collection or misuse of, or insufficient safeguards for, personal data. This provides a practical avenue for consumers affected by systemic data protection violations to pursue remedies collectively.

Although not as robust as formal class action systems, these mechanisms offer pathways for collective action in data protection cases. For instance, if a company mishandles or unlawfully processes the personal data of multiple consumers, a consumer protection association could take legal action on their behalf, ensuring access to justice and promoting accountability.

Egypt currently lacks a formal collective redress framework, but these tools indicate a growing recognition of collective interests in areas such as consumer rights and labour protections. As awareness of data protection laws increases, these mechanisms could play a significant role in addressing violations, paving the way for potential legal reforms to establish a more comprehensive system for collective redress in the future.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

IoT Regulations in Egypt

The NTRA issued the first regulatory framework addressing the IoT in January 2022. This framework aligns with Egypt's 2030 vision and the establishment of smart cities such as the New Administrative Capital. The framework outlines the objectives, scope and obligations for IoT services and data processing entities to ensure responsible use and governance of IoT technologies.

Main objectives and scope

- Facilitating IoT growth – the framework aims to advance the spread and adoption of IoT services in Egypt by removing obstacles, creating a structured regulatory environment, and fostering innovation.
- Defining IoT services – IoT is defined as a service enabling automatic communication between objects or "things" through digital/electronic identities, facilitating data exchange, analysis and processing. Examples include connected devices such as refrigerators, cars, power stations and sensors embedded in smart infrastructure.
- Classifying IoT services – IoT services are classified into five categories based on their use. For instance, "consumer applications" include devices such as wearable technology and smart home systems, allowing users to monitor and manage their homes, whereas, "commercial applications" encompass intelligent transportation systems (ITS), surveillance systems and vehicle-to-vehicle (V2V) connections.

Rights and Obligations of Data Holders and Data Processing Entities

Data holders

IoT technology mainly depends on the collection of data and its exchange, analysis and processing. Therefore, an IoT service provider is obliged to fulfil all necessary institutional and technical procedures and steps to protect the confidentiality of information and data of the service or

end users, as per the general obligations prescribed by the NTRA IoT regulatory framework, the Telecommunications Law and particularly the Data Protection Law. Therefore, the conditions discussed under **1.1 Overview of Data and Privacy-Related Laws** must be met.

Data processing entities

The NTRA IoT regulatory framework further grants several rights to data processing entities to facilitate their operation within the IoT ecosystem while ensuring regulatory compliance. Entities are allowed to establish and operate IoT platforms for personal use, subject to obtaining the necessary permits from the NTRA. Licensed IoT service providers have the right to offer IoT services to end users through agreements with network operators, in adherence with the NTRA's technical rules.

Data processing entities also have the right to own and manage the data collected through their IoT platforms, provided they implement robust organisational and technical measures to protect user information and comply with applicable data protection laws. These rights are coupled with obligations, such as obtaining legal approvals, adhering to technical standards and safeguarding national security. By balancing these rights with responsibilities, the framework supports the growth of IoT services while ensuring the protection of user data and alignment with Egypt's legal and regulatory environment.

3.2 Interaction of Data Regulation and Data Protection

The interplay between data regulation and data protection requirements in Egypt reflects a structured approach to balancing technological advancement with individual privacy rights. Data regulation frameworks such as the Telecommunications Law and the NTRA IoT regulatory framework set operational standards for the lawful collection, transmission and storage of data, ensuring that entities handling data comply with technical and procedural requirements. These regulations often apply to entities operating within specific industries, such as telecommunications or IoT service providers, with a focus on maintaining data integrity, security and lawful usage.

On the other hand, the PDPL complements these regulations by addressing the rights of individuals whose data is being processed. The PDPL ensures that personal data is handled transparently and securely, with clear obligations on data controllers and processors to obtain consent, protect data from breaches, and limit processing to legitimate and declared purposes. Together, these regulations ensure that data is managed in compliance with operational standards, and also that it is protected against misuse or unauthorised access.

A practical example of this interplay is seen in IoT services, where providers must comply with the technical requirements set out by the NTRA while ensuring adherence to PDPL safeguards. For instance, while the IoT regulatory framework mandates the secure transmission of data through authorised networks, the PDPL requires service providers to obtain explicit user consent for data collection and processing, thus ensuring both operational compliance and privacy protection.

This interplay is enforced through various regulatory bodies, such as the PDPC and the NTRA, which monitor compliance with data protection laws and operational regulations. Such co-ordination enables a comprehensive governance model that supports the growth of technology-driven services while ensuring that individual

rights are protected and legal obligations are upheld. This integrated approach fosters trust in data-driven industries and ensures that privacy and innovation can coexist harmoniously in Egypt's evolving digital ecosystem.

3.3 Rights and Obligations Under Applicable Data Regulation

IoT Regulatory Obligations

Egypt's laws governing IoT and data processing services aim to secure data handling while protecting user rights. IoT service providers and data processors must comply with licensing, data security, transparency and privacy requirements, as outlined by the NTRA IoT regulatory framework, the PDPL and related regulations.

IoT licensing in Egypt

The NTRA IoT regulatory framework outlines the licences required for IoT service providers to establish, operate and provide services, as follows.

Annex to Mobile Service Provider's Licence

This grants mobile operators the right to:

- establish IoT networks using Narrow Band IoT (NB-IoT) and LTE-m technologies;
- operate and provide IoT services via Non-Cellular LPWAN and mobile networks; and
- offer IoT connectivity services when needed.

Licence for Non-Cellular LPWAN

This is issued to non-mobile telecom operators, allowing them to:

- establish and operate Non-Cellular LPWAN; and
- provide IoT connectivity services and offer IoT services to others in Egypt using their LPWAN infrastructure.

Licence for Satellite IoT Services

This permits satellite operators to provide IoT connectivity services indirectly via licensed IoT providers. Satellite operators may not serve end users directly in Egypt but can offer IoT services through licensed networks.

IoT Service Provision Licence

This is valid for five years, renewable for an additional five years, and obliges service providers to:

- build IoT platforms and establish necessary systems for service delivery;
- use licensed telecom networks for IoT connectivity;
- obtain NTRA consent before providing services to government authorities; and
- ensure compliance with international standards and protect user data.

Licence prerequisites

The IoT regulatory framework further specifies the prerequisites and requirements for submitting a licence application. Corporations seeking any of the aforementioned licences must:

- be an Egyptian corporation established pursuant to the Egyptian Law, for which telecommunications is the core business, expect for the cases indicated by the NTRA for satellite operators;
- demonstrate reasonable telecom experience, especially in IoT services, whether through the applying corporation itself, its shareholders or affiliated companies; and
- provide proof of fiscal ability to undertake the licensed activities and meet all relevant financial obligations.

Data processors' obligations under the PDPL in the context of IoT

When applied to IoT services, the PDPL establishes specific rights and obligations for data processors, ensuring the secure and responsible handling of personal data processed by IoT devices. These obligations include:

- conducting and implementing data processing pursuant to the PDPL and its executive regulations in accordance with legitimate and legal cases and based on the provisions stipulated under the PDPC;
- ensuring the legitimacy of the purpose of the data processing and the practice thereof, and the non-violation of public order or morals;
- not exceeding the purpose and period required for data processing, and notifying the controller, the data subject or each relevant person, as the case may be, of the period necessary for the data processing;
- deleting the personal data following the lapse of the period for processing or delivering the data to the data controller;
- undertaking or refraining from undertaking an action that would result in disclosing the personal data or disclosing the outcome of the data processing;
- not undertaking 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;
- protecting and securing the processing activity, the mediums and the electronic devices used in processing, as well as the personal data thereon;
- not causing harm, whether directly or indirectly, to the data subject;
- maintaining a detailed record of data processing activities, including processing categories, contact details, the DPO, processing scope and duration, mechanisms for data deletion or modification, and descriptions of security measures and procedures;
- providing the means to prove the data processor's compliance with the provisions of the PDPL, at the request of the data controller, and enabling the PDPC to conduct inspections and supervision to ensure compliance with the provisions of the PDPL;
- obtaining a licence or permit from the PDPC in order to handle personal data; and
- appointing a local representative when the data processor is outside Egypt.

By integrating these obligations into their operations, IoT service providers can build trust with users, ensure data protection and align with Egypt's regulatory requirements for IoT and data processing activities. This ensures that, while IoT services advance connectivity and innovation, they also uphold the privacy and security of individuals' data.

3.4 Regulators and Enforcement

Bodies Enforcing Data Regulation in Egypt in Relation to IoT

National Telecommunications Regulatory Authority

The NTRA oversees the regulatory framework for IoT services, including licensing, compliance with technical standards and adherence to national security requirements. It enforces rules on data confidentiality, operational transparency and the secure handling of IoT-generated data by service providers.

Personal Data Protection Centre

Established under the PDPL, the PDPC is responsible for enforcing data protection requirements, including the processing, retention and security of personal data generated by IoT devices. The

PDPC conducts inspections, grants licences for data processing activities, and ensures compliance with privacy and data security standards.

Ministry of Telecommunications and Information Technology (MCIT)

The MCIT provides overarching supervision of IoT policy and ensures alignment with Egypt's digital transformation goals. It collaborates with the NTRA to support IoT development while safeguarding data privacy.

Consumer Protection Authority (CPA)

The CPA enforces the Consumer Protection Law, ensuring IoT service providers protect consumer rights, including the privacy and confidentiality of personal data.

These bodies work collaboratively to ensure IoT services in Egypt operate securely, comply with data regulations, and respect user privacy while advancing technological innovation.

4. Sectoral Issues

4.1 Use of Cookies

Requirements for the Use of Cookies in Egypt

Specific cookie regulations akin to those under the EU GDPR (eg, cookie banners) are not explicitly legislated in Egypt, but cookie usage falls under the broader frameworks of the PDPL and other related privacy laws, as outlined under **1.1 Overview of Data and Privacy-Related Laws**. These laws outline the following requirements for data collection and processing that apply to cookies when they involve personal data.

- Consent – cookies that collect personal data require the user's explicit consent before being deployed. This applies to cookies used for purposes beyond what is strictly necessary for the website's basic functionality, such as analytics or marketing.
- Transparency – users must be informed about the types of cookies used, their purpose, and how their data will be processed. This can be achieved through a clear and accessible cookie policy.
- Purpose limitation – cookies must only collect and process data for legitimate, declared and specific purposes. The data collected should not exceed what is necessary for these purposes.
- Right to opt-out – users must be provided with a mechanism to manage or decline non-essential cookies. This ensures compliance with the PDPL's requirement for respecting data subject rights.
- Retention and deletion – data collected through cookies must be retained only for the duration necessary to achieve the intended purpose, and deleted or anonymised thereafter.
- Security measures – website operators must implement technical and organisational measures to ensure the security of data collected through cookies, preventing unauthorised access or misuse.

Practical implementation

Website operators using cookies in Egypt should:

- provide a cookie banner or similar tool to obtain user consent before activating non-essential cookies;
- offer a cookie policy that outlines the types of cookies used, their purpose, and how users can manage or revoke consent; and
- regularly review and update cookie practices to align with the evolving regulatory environment.

By adhering to these requirements, organisations can ensure compliance with Egypt's data protection laws while building trust with their users.

4.2 Personalised Advertising and Other Online Marketing Practices

Regulation of Personalised Advertising in Egypt

The PDPL regulates direct electronic marketing, which can be considered a form of personalised advertising. Direct electronic marketing is strictly regulated under the PDPL, requiring explicit consent from data subjects before their personal data can be used for marketing purposes. Advertisers must clearly identify themselves, provide an easy opt-out mechanism, and maintain records of user consent. These regulations ensure transparency, accountability and the protection of individuals' privacy in targeted advertising practices.

Generally, Article 17 of the PDPL 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 PDPL obliges the sender of direct marketing communication to:

- specify the marketing purpose;
- not disclose the communication information to the data subject; and
- 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 Consumer Protection Law adds a further layer of protection for users exposed to personalised advertising that leads to digital transactions (eg, purchasing a product or service via an online ad). It ensures, inter alia, the following.

- Confirmation of consent – if a consumer accepts an offer made through a personalised ad, the advertiser or seller must confirm the consumer's consent to proceed with the contract.
- Right to amend or cancel – consumers have the right to modify or correct their order within seven working days of their acceptance, unless a longer period is agreed upon by both parties. This ensures flexibility and safeguards consumers from committing to contracts under unclear terms.
- Written notification of contract terms – the seller or advertiser must immediately send a written confirmation of the contract, including all details of the offer and the complete terms of the agreement. This notification can be sent via email or another storable electronic medium, and must not contain terms or details that differ from the original offer made in the personalised ad.
- Transparency and accuracy – advertisers and sellers are prohibited from including misleading or inconsistent information in the contract confirmation compared to the original advertisement, ensuring consumers are fully informed.

Therefore, the regulatory framework in Egypt ensures that personalised advertising aligns with user privacy and consumer rights. While the PDPL focuses on securing consent, transparency and accountability in marketing communications, the Consumer Protection Law reinforces these protections in the next stage, when personalised advertising leads to online contracts. By adhering to these standards, advertisers can foster trust and avoid legal risks while engaging in targeted digital marketing.

4.3 Employment Privacy Law

The Effect of Data Privacy Law on the Employment Relationship in Egypt

The PDPL applies broadly to all personal data, including in the context of employment relationships. It imposes clear obligations on employers concerning the collection, processing and retention of employee personal data, while granting employees extensive rights to control and protect their information. This fosters a culture of transparency and accountability within the workplace. Consequently, the conditions outlined under **1.1 Overview of Data and Privacy-Related Laws** must be adhered to.

Employers' obligations under the PDPL and Labour Law

Employers are subject to several obligations and conditions when handling employees' personal data, as outlined in the PDPL and Labour Law as follows.

- Legitimate data collection – employers must collect personal data for legitimate, specific and declared purposes related to the employment relationship, such as performance evaluations, disciplinary actions or payroll processing.
- Data accuracy and security – employers are required to ensure that the personal data they collect is correct, secure and processed lawfully, protecting it from unauthorised access or breaches.
- Retention periods – the PDPL restricts employers from retaining personal data for longer than necessary for the declared purposes. The Labour Law No 12/2003 ("Labour Law") further stipulates that employers must retain employees' files for at least one year after termination.
- File creation and maintenance – employers must create a detailed file for each employee, including information such as their name, job title, marital status, salary, leave records, disciplinary actions and performance evaluations. Access to these files is restricted to those authorised by law.

Accordingly, the PDPL has introduced a significant shift in employment relationships in Egypt by safeguarding employees' privacy rights and imposing strict obligations on employers. By aligning their practices with the PDPL and Labour Law, employers can ensure compliance while maintaining a transparent and respectful relationship with their workforce. This legal framework not only enhances employee confidence but also promotes a fair and accountable workplace environment.

4.4 Transfer of Personal Data in Asset Deals

Requirements for Data Processing in the Course of Asset Deals in Egypt

While the PDPL does not explicitly address data processing in the context of asset deals, its general principles and requirements for personal data protection apply. These regulations govern the lawful handling of personal data during transactions such as transfers of business assets, ensuring compliance with privacy standards.

Consent and legal basis
Although not explicitly mentioned for asset deals, the PDPL requires personal data to be processed only with the explicit consent of the data subjects.

Personal data must be processed for legitimate and declared purposes directly related to the asset deal, such as due diligence or transaction implementation.

Transparency and notification
Data subjects should be informed about the nature of the transaction, the purpose of data processing, the identity of the acquiring party, and any potential impact on their privacy rights.

Data security
Entities must implement robust security measures to ensure personal data is protected during the transfer process, preventing unauthorised access or breaches.

Personal data should only be accessible to authorised individuals directly involved in the transaction.

Retention and deletion
Data should only be retained for the duration necessary to complete the transaction or fulfil legal requirements.

Any redundant or unnecessary data must be securely deleted after the transaction is finalised, unless retention is required by law.

Compliance with data subject's rights
Data subjects retain the right to access, correct or delete their data. They may also object to its processing if it conflicts with their fundamental rights and freedoms.

Data subjects must be notified of any breach involving their personal data.

Third-party agreements
If third-party advisers or consultants are involved, clear data-sharing agreements must be established to ensure confidentiality and compliance with the PDPL.

Although the PDPL does not explicitly address data processing during asset deals, its general principles apply to ensure the lawful and secure handling of personal data. By adhering to the PDPL's requirements for consent, security and transparency, parties can manage personal data responsibly during such transactions while minimising legal risks.

5. International Considerations

5.1 Restrictions on International Data Transfers

The PDPL 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.

Articles (14–16) of the PDPL are concerned with the 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 PDPC, which will be established pursuant to Articles 19–25 of the PDPL. Consequently, if the level of protection is found adequate and conforms with that of the PDPL, a licence or permit will be granted by the PDPC in order to be able to transfer the data.

5.2 Government Notifications and Approvals

Approvals Required for Cross-Border Data Transfer

The PDPC's approval is required to obtain a licence or permit to proceed with transferring data across borders. In order to apply for said licence or permit, an application must be submitted on the forms produced by the PDPC and attaching all the necessary supporting materials, demonstrating the applicant's financial stability and technical competence. Following the completion of all the applications, decisions must be made within 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 PDPC.

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

It is worth mentioning that the PDPC, 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 that 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 PDPL.

This framework ensures that international data transfers comply with Egypt's commitment to safeguarding personal data and maintaining regulatory oversight.

5.3 Data Localisation Requirements

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

Said data centres require specific licences in order to be registered and able to operate, which 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, but 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, but registration as a CSP is required when operating inside Egypt.

5.4 Blocking Statutes

Prior to the issuance of Press and Media Regulations Law No 180/2018 (the "Media Law"), the Egyptian Constitution prohibited the imposition of censorship over Egyptian newspapers and media outlets, or the confiscation, suspension or closing of 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 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 the "blocking" of various media content.

Accordingly, after 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 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.

5.5 Recent Developments

International Transfer of Personal Data

The regulation of international data transfers in Egypt has evolved with the introduction of the PDPL, which establishes strict requirements for transferring personal data across borders. The law mandates prior approval from the PDPC for any cross-border transfers, unless specific exceptions apply. While the PDPL's executive regulations are still pending, they are expected to provide detailed procedures for applying for PDPC approval, criteria for adequacy decisions, and requirements for mitigating high-risk transfers.

Sector-specific regulations such as the Banking Law No 194/2020 and the Telecommunications Law introduce additional restrictions on the international transfer of sensitive data within their respective domains, reinforcing Egypt's commitment to data sovereignty and security. In this regard, the Banking Law prohibits the sharing of customer financial data with foreign entities without prior regulatory approval, while the Telecommunications Law restricts the transfer of telecommunications-related data outside Egypt unless explicitly authorised. These measures align Egypt's regulatory framework with global data protection standards while prioritising the protection of individual privacy and national interests.