EGYPT

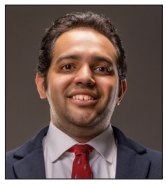
Law and Practice

Contributed by:
Ibrahim Shehata, Salah Mohamed, Hana Elbarbary and Hamza Shehata
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 result-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 law firm, then moved to Sharkawy & Sarhan law firm. Earlier in his career, he focused on corporate law and successfully advised several multinational companies on doing business in Egypt. In recent 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 guiding them to be more investment-ready. Ibrahim has an LLM in International Arbitration and Venture Capital from New York University.

Salah Mohamed joined Shehata & Partners as an associate in 2023, having previously worked as an intern at several top-tier law firms in Egypt. Salah is actively involved in reviewing and drafting different types of legal contracts, including SAFEs, convertible notes, shareholder agreements, term sheets and those relating to employment matters.

Hana Elbarbary has recently joined Shehata & Partners. She holds a French LLB from Sorbonne University's Institut de Droit des Affaires Internationales (IDAI) and an Egyptian LLB from Cairo University. She is further advancing her expertise by pursuing a Master's degree in international business law at Sorbonne University's IDAI. Hana has substantial experience in corporate and competition law at top-tier Egyptian law firms, where she has played an important role in navigating complex legal challenges and contributed to important cases in both fields.

Hamza Shehata has recently joined Shehata & Partners as a junior associate following his graduation from Cairo University's Faculty of Law (English Section). During his internships at top-tier law firms, Hamza gained valuable experience working on corporate, litigation and arbitration matters, primarily focusing on employment law.

Shehata & Partners

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

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

1. Data Privacy Regulations

1.1 Data Privacy and Cloud Computing

The National Telecommunications Regulatory Authority (NTRA) has set in place a regulatory framework for establishing and operating data centres and providing hosting and cloud computing services.

This regulatory framework was created to attract large-scale data centres, cloud computing service providers, and electronic content providers to the Egyptian market. Its goal is to support Egypt's digital transformation efforts as well as facilitate the delivery of cutting-edge electronic services to citizens.

This framework instils the requirements for establishing and operating data centres, as well as providing hosting and cloud computing services. According to this framework, there are several factors that determine whether it is required to obtain a licence from the NTRA or if a simpler registration process is sufficient.

This framework indicates that the requirements to establish and operate data centres and provide cloud computing services may vary depending on three factors:

- the geographical location of the beneficiary clients;
- the type of service delivered to beneficiaries; and
- the scope of work of the beneficiary client.

More specifically, the scope of beneficiaries varies based on whether the services are restricted to supporting the provider's internal activities or extends to other beneficiaries.

However, the relatively new nature of this regulatory framework has made it that it merely indicates the foregoing details, without defining personal and sensitive data or how it is processed in the cloud. It merely indicates that entities that provide various cloud computing services, either through fully owned data centres or rented data centres, are required to register with the NTRA as a cloud service provider if they are located in Egypt. However, there are no such requirements for licences or registration with the NTRA for entities located outside of Egypt.

Nonetheless, the Egyptian Data Protection Law No 151 of 2020 (DPL) regulates how personal information is collected, processed, stored and shared within Egypt. The stipulations of this Law address various general aspects of data privacy, including consent, data subject rights, data security and cross-border data transfers, thereby ensuring a transparent framework that regulates how data is handled. The DPL is currently the only Egyptian legislation that provides a general definition of personal and sensitive data, however, it is not necessarily applicable to a cloud environment. In other words, the aforementioned NTRA framework does not define personal or sensitive data, however the DPL defines personal data as any information related to an individual who is either already identified or can be identified, directly or indirectly, by linking that information with other details such as name, voice, identification number, or data regarding psychological or physical health, among others. Additionally, sensitive data is defined under the DPL as any personal information that discloses details about a person's psychological, mental or physical health, religious beliefs, political opinions and similar attributes.

It is important to note that these definitions are not specific to cloud computing service providers, therefore it is not certain whether this definition will be adopted by the NTRA for cloud computing service providers or not.

In regards to the specific requirements for processing personal data in the cloud, a cloud service provider that is located in Egypt must do the following in order to register with the NTRA to obtain their approval and become a licensed cloud service provider in Egypt:

- provide the complete data related to the entity's information (name of the entity, address, phone numbers, commercial register, contact points, etc); and
- provide the complete data related to the nature of the activity (services), more specifically, the hosting system used, the data centres located in Egypt, their full address and contact details (telephone/fax/e-mail), and the entity's website URL.

1.2 Data Privacy and Cross-Border Transfers

Cross-Border Data Transfers

Egypt regulates cross-border data transfers by virtue of its DPL. The DPL sets in place strict rules to ensure that personal data shared with other countries is protected to a high standard. According to Article 14 of the DPL, transferring, storing or sharing personal data with a foreign country is generally prohibited unless that country offers protection equal to or greater than what is required by Egyptian law. Additionally, such transfers need a licence or permit from the Egyptian Data Protection Centre (DPC).

Exceptions

However, Article 15 indicates that there are several exceptions where data can be transferred even if the receiving country does not meet these protection standards, provided that the data subject or their representative consent to it. These exceptions include situations where transferring data is necessary to protect someone's life, provide medical care or manage health services. It also covers cases where the data is needed to fulfil legal obligations, execute or conclude contracts benefiting the data subject, or support international judicial co-operation. Additionally, transfers are permitted for public interest reasons, financial transactions in accordance with national laws of the other country, or when required by international agreements that Egypt is party to.

1.3 Penalties for Non-compliance With Data Privacy Regulations

Penalties

The DPL indicates specific penalties for different kinds of violations that could occur. Although the DPL enforces strict data privacy rules, it does not specifically cover cloud computing and related regulations. Therefore, the only existing penalties under the Egyptian legal system are currently the ones indicated in the DPL. The goal of these penalties is to ensure that anyone handling personal data, whether they are a natural or juristic person, follows the law and respects privacy rights. In this context, according to Article 30 of the DPL, without prejudice to any civil or criminal liability, if a violation occurs, the CEO of the DPC can issue a warning to the violator, who is usually either a controller or a processor, and then grant them a set time to comply with the DPL provisions. If the violator does not comply, the DPC Board of Directors (BoD) can take more serious steps, such as partially or fully suspending or even cancelling licences or permits. They can also publicly disclose the violations that have been proven to have occurred in one or more popular media outlets, or even place the violator under technical supervision of the centre, all at the expense of the violator.

Monetary Fines

Moreover, Articles No 36 and 37 of the DPL indicate that any violations of the data protection measures indicated by the law shall be penalised with a fine of between EGP100,000 and EGP1 million. Not to mention, if this violation was committed in exchange for material or moral benefit, or with the intention of inflicting harm on the data subject, the penalty is imprisonment for a minimum period of six months and a fine of between EGP200,000 and EGP2 million, or one of these penalties.

Penalties for Handling Sensitive Data

Lastly, Article 41 of the DPL specifically mentions that anyone who handles sensitive data, whether they are collecting, sharing, storing or granting access to it, without the explicit consent of the data subject, and outside the legally authorised situations, faces serious legal consequences. More specifically, those found guilty of such violations can be sentenced to at least three months' imprisonment. Additionally, they may be fined between EGP500,000 and EGP5 million. The DPL allows for either imprisonment, a fine, or both as penalties, depending on the severity of the violation.

2. Data Security Measures

2.1 Data Security and the Cloud

The NTRA has set in place a regulatory framework that specifically outlines the steps and requirements for establishing and operating data centres and providing hosting and cloud computing services. However, there are still lots of issues related to the topic of security measures for data stored in the cloud that are yet to be addressed by the NTRA.

The DPL does not specifically mention any security measures that specifically pertain to data stored in the cloud. It does, however, mention certain general obligations and conditions for data processing, which covers data storage as it is one of the stages of data processing.

The Legitimacy of the Data Processing

Under Article 6 of the DPL, data processing is considered legitimate and lawful when it meets certain criteria, such as obtaining the data subject's consent for specific purposes, fulfilling contractual obligations, or complying with a legal order, such as implementing an obligation

regulated by DPL, an order from the competent investigation authorities or a judicial ruling. It also allows the processing of the controller's legitimate rights as long as it does not infringe on the fundamental rights and freedoms of the data subject.

The Data Protection Officer

Moreover, Article 8 of the DPL requires organisations to appoint a specialised employee responsible for data protection, who must be registered with a special registry with the DPC. This employee, known as the data protection officer (DPO), is responsible for implementing the provisions of the DPL, conducting regular evaluations and acting as a point of contact with the DPC.

The DPO's Responsibilities

Additionally, as a measure to ensure the protection of data, Article 9 of the DPL further indicates the responsibilities of the DPO, including monitoring compliance within their organisation, documenting evaluations, and responding to requests related to personal data. The DPO shall also notify the DPC of any data breaches and ensure that violations are addressed promptly.

Adoption of Security Measures

Article 10 of the DPL addresses the need for data controllers and processors to adopt security measures that are proportional to the risks involved in data processing disclosure. This includes preventing unauthorised access, the disclosure or the destruction of data. When receiving personal data disclosure requests, controllers and processors must adhere to specific procedures, such as verifying the legitimacy of the request, obtaining the required documents and responding within a set timeframe of six days. Additionally, should this request be declined, the refusal must be accompanied by a rationale.

The Conditions for Processing Personal Data

Article 12 of the DPL outlines the conditions for processing personal data, including obtaining a licence from the DPC and the consent of the data subject, especially when dealing with sensitive data or data related to children.

The Importance of Data Security and Confidentiality

Additionally, Articles 7, 14 and 15 of the DPL reinforce the importance of data security and confidentiality, mandating that personal data be processed securely and in line with the DPL principles. The DPL also addresses encryption, particularly in transit, to protect data from interception during transfer.

The Transfer of Personal Data

Article 16 allows the transfer of personal data outside Egypt with a licence from the DPC, provided certain conditions are met, such as ensuring that the foreign entity offers comparable protection standards as mentioned in **6.1 Cross-Border Transfer Regulation**.

Penalties for Data Breaches

Moreover, as part of the security measures enforced by the DPL, there are also strict penalties for data breaches, as outlined in Article 30. Violators may face licence suspension, fines and even public disclosure of their violations. The DPL also requires immediate notification to the DPC of data breaches, with specific details on how to report such incidents. Furthermore, the DPO is responsible for ensuring that data subjects are informed of any breaches. All of these measures highlight the extent to which the DPL aims to safeguard data privacy.

The Right to File Complaints

Lastly, Article 33 of the DPL gives data subjects the right to file complaints if their data protec-

tion rights are violated. Consequently, the DPC shall investigate these complaints and issue a decision within 30 days, obligating the offender to adhere to the DPC's decision without delay.

3. Data Ownership and Control

3.1 Data Ownership in Cloud Agreements

As mentioned in **1.1 Data Privacy and Cloud Computing**, the NTRA has established a regulatory framework that outlines the steps and requirements for establishing and operating data centres and providing hosting and cloud computing services. However, this framework does not cover the topic of data ownership in cloud agreements.

With that being said, the only applicable legislation on this matter is the DPL, which generally addresses the topic of data ownership and grants individuals several important rights concerning their personal data. In this regard, Article 2 of the DPL stipulates that the data subjects have the right to access, obtain, and be informed about their personal data held by any entity. They can also withdraw consent for the retention or processing of their data and request the correction, modification, erasure or updating of their personal information. Additionally, they can limit the processing of their data to a specific scope, and must be informed if there is any breach or violation of their data.

Moreover, the data subjects have the right to object to data processing if it conflicts with their fundamental rights and freedoms. In this context, Article 32 of the DPL stipulates that the data subjects can submit a request(s) to any entity holding, controlling or processing their data to exercise these rights, and the entity must respond within six working days.

Furthermore, without prejudice to the right of recourse to litigation, Article 33 of the DPL outlines that individuals can file complaints to the DPC in cases where their data protection rights are violated, they are prevented from exercising their rights, or they disagree with decisions made by the data controller or processor. Accordingly, the DPC must investigate and issue a decision within 30 business days. The entity against whom the complaint is made must implement the DPC's decision within seven business days of being notified.

3.2 Data Portability

There are currently no clear provisions that concern data portability and the measures that should be taken for data portability, other than those listed in the DPL and the cloud computing regulatory framework issued by the NTRA.

According to Article 15 of the DPL, personal data can be transferred, shared, traded or processed in a country that may not offer the same level of data protection as Egypt, under certain conditions. These conditions include obtaining explicit consent from the data subject or their legal representative for the transfer of their personal data. Additionally, the transfer is permitted when it is necessary to protect the life of the data subject, to provide medical care, to manage health services, or to ensure appropriate treatment. The DPL also allows for data transfer to fulfil legal obligations that ensure a right is established, exercised or defended before judicial authorities.

Moreover, the transfer is permissible if it is required to conclude, implement or prepare a contract between the data controller or proces-

sor and a third party that benefits the data subject.

Furthermore, Article 16 of the DPL specifies that a data controller or processor in Egypt may transfer personal data to an entity outside the country if they first obtain a licence from the DPC. This is only allowed if the roles and responsibilities of the controllers or processors are clearly defined, there is a legitimate interest for all parties involved, and the legal and technical protection for the data in the foreign country is at least equivalent to the protection provided in Egypt. More specifically, the NTRA considers that cloud computing services offered by foreign entities intended for end-users in Egypt are categorised as services provided by a private data centre. This classification is based on the fact that a foreign entity will not offer these services to third parties, but will exclusively offer it to its own end-users.

3.3 Data Retention and Deletion

In Egypt, the concept of data retention and deletion in cloud environments is not specifically addressed by any existing laws or regulations, not even the NTRA's regulatory framework for cloud computing. However, the DPL provides some guidance on data retention and deletion. The DPL refers to this process as a "processing process." According to Article 1 of the DPL, this process includes any electronic or technical activity related to writing, collecting, recording, saving or erasing personal data. This can involve various types of media or devices, whether the process is done partially or fully. Although the DPL states that specific policies and procedures for data processing should be detailed in the DPL Executive Regulations, these Regulations have not yet been published, and the DPL does not explicitly cover these aspects when it comes to cloud governance.

Rules for Handling Data Processing

However, the DPL does lay out some important rules for how data processing should be handled. For instance, Articles 2 and 6 make it clear that personal data cannot be processed without the explicit consent of the data subjects. Additionally, Article 2 of the DPL gives data subjects the right to have their personal data modified, deleted or corrected if needed. Moreover, Article 4 also requires data controllers to erase personal data as soon as it has served the purpose for which it was collected.

Additionally, Articles 4 (10) and 5 (11) of the DPL require both data controllers and processors to obtain the necessary licences and permits from the DPC before they can legally process any personal data. Accordingly, Article 26 (2) of the DPL further emphasises that the DPC is responsible for issuing these licences and permits, which are needed for data storage, processing and related operations under the provisions of the DPL.

4. Vendor Management

4.1 Due Diligence

The Cloud Service Provider

When selecting a cloud service provider, it is crucial to make sure they have completed the registration procedures with the NTRA and that they have obtained a licence from that entity to provide their services. The NTRA enforces stringent registration requirements. These requirements include evaluations of the provider's cybersecurity systems, with the necessity to obtain an accreditation certificate from the NTRA. This rigorous regulatory framework ensures that the cloud service providers operating within Egypt meet the highest standards of security and reliability, providing a robust level of safety and compliance.

Registration for Cloud Service Providers

The NTRA mandates a very detailed and structured registration process for a cloud service provider. This procedure is detailed and well structured as it makes sure that all operations are conducted securely.

The registration is valid for a period of 15 years, during which the provider is granted specific rights and must adhere to particular obligations. To begin, the registration process requires the approval of the NTRA. The applicant must first provide comprehensive entity data, including the name of the entity, its physical address, phone numbers and commercial registration details. Additionally, they must identify contact points within the organisation who will be responsible for communication with the NTRA. Beyond these basic details, the entity is also required to submit further information related to the nature of the cloud services it intends to provide. This includes specifics about the hosting system they will use, detailed descriptions of the data centres located in Egypt (including their addresses and contact details) and the entity's website information.

Upon successful registration, the entity gains the right to provide cloud computing services, either for its own use or for other clients in Egypt. The entity will also be allowed to connect to submarine cable systems through infrastructure service providers without needing further approval from the NTRA. However, these rights come with the obligation to ensure safe cybersecurity measures. In this regard, the entity must evaluate its cybersecurity systems and obtain an accreditation certificate from the NTRA to confirm that these systems meet the required standards.

4.2 Data Protection in Cloud Service Agreements

Cloud Service Agreements

Considering how relatively new cloud services are in Egypt, the only relevant legal framework currently available is the DPL, which provides general guidance on data protection.

Requirements From the DPL

The DPL requires that explicit consent be obtained from data subjects before their information is processed. Consequently, the agreements should also detail the purposes of the data collection, the retention period and the procedures for deleting data once it is no longer needed. Additionally, cloud service providers are required to notify the data controller, the DPC and the DPO within 72 hours in the case of a data breach or immediately if the breach is related to national security.

Moreover, Article 8 of the DPL mandates that the DPO must be appointed for any legal entity that processes large volumes of data, in order to ensure compliance with all the data protection measures instilled by the DPL. Additionally, the DPC, by virtue of the DPL, has the authority to conduct inspections on the relevant entities to ensure their compliance with the provisions of the DPL.

Regarding the measures set in place to ensure compliance with data privacy regulations, the DPL has set forth significant penalties for non-compliance, including monetary fines and potential criminal liability, and this is without prejudice to any other civil or criminal liability.

4.3 Data Processing Agreements and the Cloud

There is currently no specific framework that determines how a data processing agreement

should be structured in a cloud environment. However, the data processing agreements in the cloud environment must be in compliance with the DPL. In this regard, the DPL mandates specific requirements for processing personal data, which must be incorporated into these agreements.

The Definitions of the Data Processing Agreements

The agreements shall include the same definitions and terms identified in Article 1 of the DPL, such as "the personal data, the data processing, the data controller, the data processor, etc."

The Roles of Each Party in the Data Processing Agreements

The roles of the parties must also follow the same nature that is stipulated in Article 5 of the DPL. This implies that, in accordance with the DPL, the agreements must specify that the data controller establishes the objectives and methods of processing, while the data processor handles the data on behalf of the controller.

The Nature of Data Processing Activities

The nature of the data processing activities shall be clearly indicated in the contract and must conform to the purposes mentioned in Article 5 of the DPL, detailing the specific obligations of data processors. Consequently, the DPL stipulates that personal data should only be processed for specific and clear purposes, and the agreement should abide by these instructions by not allowing any other kinds of activities.

The Necessary Measures in the Event of a Data Breach

Article 7 of DPL outlines the importance of the procedures to be followed in the event of a data breach. Consequently, the agreement should implement these measures, which indicates that the processor shall safeguard personal data against any threats, including data breaches.

The Data Subjects Rights Under the DPL

Lastly, Articles 2 and 3 of the DPL ensure that data subjects have certain rights, such as accessing their data, requesting corrections, and having their data deleted when necessary, therefore these rights should also be taken into consideration when drafting the provisions of such agreements.

4.4 Exit Strategies and Data Migration

Given how cloud computing is still in the developmental stage in Egypt, the NTRA has set in place a regulatory framework that specifically outlines the steps and requirements for establishing and operating data centres and providing hosting and cloud computing services. However, the topic of termination and exit strategies for cloud service agreements is yet to be addressed by the NTRA or the DPL Executive Regulations as no legislation currently covers this topic.

These agreements are therefore subject to the general stipulations of Law No 131 of 1948, as amended (ECC), which governs the contract formation, execution and termination based on the mutual consent and intent of the contracting parties.

5. Data Breach Notification

5.1 Requirements to Report Data Breaches

Data Breaches in the Cloud Environment

In Egypt, the concept of data breaches in cloud environments is not specifically addressed by the cloud computing regulatory framework issued by the NTRA. However, there is an applicable legal framework that is currently available,

which is the DPL, which provides general guidance on data breaches and violations. Under Article 1, a data breach or violation is defined as any unauthorised or illegal access to personal data. This includes not only accessing the data without permission but also copying, sending, distributing, exchanging, transmitting or circulating the data with the intention of revealing, disclosing, destroying or altering it, whether the data is being stored, transferred or processed at the time.

Procedures for Reporting Data Breaches

The DPL establishes specific procedures for reporting data breaches. In this regard, Article 7 of the DPL stipulates that both the data controller and the data processor shall notify the DPC within 72 hours of becoming aware of a breach or violation or immediately if such breach is related to national security. Additionally, the data subject must be informed within three days of the breach being reported to the DPC.

Report Contents

The report must include:

- a description of the nature, form and causes of the breach or violation, as well as an estimate of the number of affected personal data records;
- the contact details of the personal data protection officer;
- an assessment of the potential impacts of the breach or violation;
- a detailed description of the measures that have been taken or are planned to address the breach or violation and mitigate its effects; and
- documentation of the breach or violation and the corrective actions taken.

Moreover, the failure to comply with these reporting requirements, as stipulated in Article 7 of the DPL, may result in significant fines. In this context, Article 38 of the DPL states that the data controller or the processor who does not fulfil these duties can be fined between EGP300,000 and EGP3 million.

Additionally, Article 9 of the DPL places responsibility on the DPO to notify the DPC of any breaches or violations of personal data. If the DPO fails to do so, the DPO could face a fine ranging from EGP200,000 to EGP2 million. If the breach occurs due to the negligence of the DPO, the penalty could be a fine between EGP50,000 and EGP500,000.

Lastly, Article 33 of the DPL grants data subjects whose data has been compromised the right to file a complaint with the DPC. The DPC is then required to investigate the complaint and issue a decision within 30 business days. Both the complainant and the accused party must be informed of the decision. The party against whom the complaint was made is required to comply with the decision of the DPC within seven business days of being notified and shall also inform the DPC of the actions taken to implement the decision.

5.2 Investigating and Remedying Data Breaches

As previously mentioned, Article 33 of the DPL outlines the required procedures for handling complaints related to data breaches. Prior to the investigation of a data breach, a complaint must be submitted to the DPC, which is the authority in charge of ensuring the applicability of the DPL. Once a complaint is submitted to the DPC, the DPC is required to carry out the necessary investigations and issue a decision within 30 business days. Additionally, both the person

who filed the complaint and the person or entity being complained about must be informed of the decision of the DPC. Furthermore, the individual or the legal entity that the complaint was made against is then required to implement the decision of the DPC within seven business days of being notified. They must also inform the DPC about the actions they have taken to comply with the decision.

On another note, Article 49 of the DPL offers a provision for reconciliation in the event of a violation of Articles 36-43 of the DPL, prior to the issuance of a final ruling on a data breach case. The accused party has the opportunity to settle with the victim, but this must be done with the approval of the DPC, and it can take place before the public prosecution or the competent court. Moreover, reconciliation is permitted at any stage in the event of a violation of Articles 42, 44, and 45 of the DPL. In all cases, to achieve this reconciliation, the accused party shall pay an amount equal to half of the minimum fine prescribed for the offence. The payment shall be made subsequent to the filing of the lawsuit and prior to the court judgment becoming final. It is worth mentioning that the money can be deposited in the treasury of the competent court, the public prosecution or the DPC, depending on the situation.

5.3 Notifying Data Breaches

In Egypt, the concept of data breaches in cloud environments is not specifically addressed by any legislation, as the Egyptian cloud strategy is still relatively new and does not cover this topic in detail. However, the DPL provides general guidance on data breaches and violations. Based on that, according to Article 7 of the DPL, data controllers and processors must report any breach or violation of personal data to the DPC within 72 hours of discovering the issue. If the breach is related to national security, they are required to report it to the DPC immediately. Additionally, they must inform the affected data subjects within three days. Although Article 9 (4) does not specify precise timelines for reporting to the DPC, it designates the DPO as responsible for notifying the DPC in the event of any data breach or violation.

It is worth mentioning that, when reporting a breach of data privacy, the reports shall include specific information, such as a description of the breach or violation, including its nature, form, causes and the estimated number of personal data records affected. Moreover, the reports should also provide the contact information for the DPO, outline the potential impacts of the breach on the affected individuals, and detail the measures taken and planned to address the breach and minimise its negative effects.

6. International Data Transfers

6.1 Cross-Border Transfer Regulation

International Data Transfer

International data transfer refers to the movement of data across national borders from one country to another. This involves transferring data from one jurisdiction with specific data protection laws to another.

In this context, Articles 14, 15, and 16 of the DPL address this matter as they restrict the international transfer of data to countries whose security measures are not at the same level or fall below the Egyptian data protection security measures. Nevertheless, the approval/authorisation of the DPC is also required.

In this context, Article 15 of the DPL states that, if the entity acquires the written consent of the

person whom the data concerns, the data can be transferred internationally even if the other country's data protection measures are less rigorous than the Egyptian standards in the following cases:

- to protect the life of the data subject and provide them with medical care or treatment or the operation of health service;
- to perform obligations in order to prove the existence of a legal right or to exercise or defend such right before the judiciary;
- to fulfil or execute an agreement entered into or, to be entered into, between the data processor and third parties, for the benefit of the data subject;
- to perform a procedure relating to international judicial co-operation;
- when necessary, or required by law, in order to protect the public interest;
- to transfer money to another country pursuant to the laws of that country which are specific and in force; and
- if the transfer or circulation is pursuant to a bilateral or multilateral international agreement that Egypt is a party to.

Further, Article 16 of the DPL states that the controller or the data processor may grant access to personal data to another data controller or data processor outside the Arab Republic of Egypt by virtue of a licence from the DPC provided that the following conditions have been met:

- if there is conformity in the nature of work between the data controllers and the data processors, or unity between the purpose for which they obtain the personal data;
- if either the data controller, the data processor or the data subject has a legitimate interest in the personal data; and
- the level of legal and technical protection of the personal data offered by the controller or processor abroad shall not fall below the level of protection provided in the Arab Republic of Egypt.

Article 14 of DPL states that the mechanisms of data transferring shall be addressed in the Executive Regulations of the DPL, however, these have not yet been issued.

Data Transfer in International Agreements

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, such as 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 was signed in 1998. The scope of assistance between the contracting parties is specified under Article 1, stating that "[t]he 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."

- The Arab Convention on Combating Information Technology Offences entered into force in Egypt by the issuance of Presidential Decree No 276 for 2014. The Fourth Chapter regulates the legal and judicial assistance between the parties. In particular, Articles 38, 39, 40, 41 and 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, aims at curbing tax evasion by US citizens and residents through the use of offshore accounts operating outside the USA. 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 in 2005. Its 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. Its 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 […]." Its 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. Its 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. Its Articles 12, 13 and 14 states 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.

6.2 Data Localisation

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 in 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, as previously discussed (see **1.1 Data Privacy and Cloud Computing** and **4.1 Due Diligence**).

6.3 Conflicts of Law

Conflict of Law

A conflict of law occurs when the data protection laws of two or more countries differ or contradict each other, creating uncertainty over which rules apply to the transfer, storage or processing of personal data. In this regard, Article No (14) of the DPL prohibits the cross-border transfer of data unless the country that will receive the data has at least the same data protection standards in Egypt.

However, there are some exceptions to what is required under Article 14 of the DPL. Those exceptions are listed in Article 15 of the DPL, which concerns cross-border data transfer.

Risks and Challenges Associated with International Data Transfers in the Cloud

Risks and challenges facing data transfers are innumerable, as risks and challenges vary from technical to legal issues, issues related to to human error in a certain country, or an official deadlock and administrative problems.

The risk of a data breach and inadequate protections may be the most concerning security risks, as a country's articles may give the illusion of adequate data protection measures while the reality may vary. Furthermore, the issuance of the Executive Regulations is necessary, in order to outline the necessary provisions which relate to data privacy compliance in Egypt.

7. Compliance and Audits

7.1 Cloud Computing and Compliance/Audits

Cloud Compliance/Audits

A cloud audit is a process that systematically reviews and assesses an organisation's cloud infrastructure, security controls and compliance posture. It is a comprehensive evaluation that examines the cloud provider's security practices, data access controls and overall risk management strategies. The primary purpose of a cloud audit is to ensure that an organisation's cloud environment meets industry-specific regulatory

requirements, adheres to established security standards and effectively mitigates potential risks. In this regard, there are currently no explicit rules governing the cloud audit in Egypt. However, generally speaking, the DPL mainly gives the responsibility of conducting the compliance and audits to the DPO and the DPC.

In this context, Article 9 of the DPL states that the responsibilities of the DPO are as follows: "[To p]erform a regular evaluation and inspection of the personal data protection system and prevent its breach as well as certify the results of such evaluation and issue the necessary recommendations for its protection." This Article does not address the auditing responsibilities directly, but it is considered to be one of the applications of auditing; the Executive Regulations of the DPL that are yet to be issued shall stipulate the other responsibilities of the DPO and explain the DPO's current responsibilities in a comprehensive manner.

Furthermore, 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 pre-approval 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);
- being informed of any breach or violation of their personal data; and
- objecting to the data processing or outcome thereof if this contradicts the basic rights and freedoms of the data subject.

In addition to the data subject's 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:

- administrative liability;
- civil liability; and
- criminal liability (as applicable).

Conducting Compliance Audits and Key Areas for Focus

Audits are typically of a different nature and the type of audit will depend on the purpose thereof. As the DPL does not mention the different types of audits, it is expected that the Executive Regulations of the DPL will tackle this point in detail.

Measures to Ensure the Integrity of Audit Reports

Article 40 of the DPL states that the DPO shall be penalised by a fine not less than EGP200,000 and not exceeding EGP2 million if the DPO breaches their responsibilities stipulated in Article 9 of the DPL, which includes the DPO's responsibility of conducting an audit.

Audit Findings and Recommendations

The process of applying the recommendations and findings differs from one jurisdiction to another. Accordingly, this is not yet settled under the current provisions of the DPL.

Statutory Penalties for Failing to Comply with Audit Requirements

There are currently no clear provisions for failing to comply with the audit requirements. However, there are certain penalties listed in the DPL that concern any data breach under the DPL provisions; see **1.3 Penalties for Non-Compliance with Data Privacy Regulations**. It is worth mentioning that the upcoming DPL Executive Regulations may stipulate additional penalties concerning the data breach and the incompliance with the audit requirements.