Baker McKenzie.

InsightPlus

September 2020

In brief

After several years of debate, the Egyptian government has introduced the Republic's first standalone data protection law, which aims to regulate and protect citizens' data online. On 15 July 2020, Resolution No. 151 of 2020 (the **Law**) (available in Arabic here) was published in the Official Gazette. The provisions under the new Law are modeled on the EU General Data Protection Regulation (**GDPR**) and the Law adopts similar concepts and definitions. It is hoped that the new Law will help Egypt attract foreign investment by increasing consumer confidence in electronic data processing and setting clear parameters for companies looking to capitalise on the growth of the digital economy.

The Law will enter into force three months from when it was published in the Official Gazette (namely, on 15 October 2020). As part of the new Law, the Minister of Communications and Information Technology will issue the Law's Regulation (**Regulation**) within a further six months from the date on which the Law enters into force in Egypt. The Regulation will provide further detail on the role of the new regulator and how it will implement the new Law. Companies will have a 12-month grace period to comply with the Law from the date of publication of the Regulation (i.e., compliance is expected to be required within a minimum of 18 months from 15 October 2020, if the Regulation is issued effectively within 6 months. It may take longer to issue the Regulation).

In this alert we provide an overview of key provisions in order to help businesses prepare for the enforcement of the new Law.

Key takeaways

- The Law is effective from 15 October 2020 and companies will have at least 18 months from this date to become compliant.
- The grace period allows Egyptian national companies a generous period of time to consider the Law's impact and to put in place an appropriate compliance program, given that many of the requirements will be entirely new to them.
- The Law imposes obligations on both data controllers and data processors, although many of the obligations imposed directly on

Contact information

Ghada El Ehwany
Partner
Cairo
Ghada.ElEhwany
@bakermckenzie.com

Kelli Blyth
Counsel
Dubai
Kellie.Blyth
@bakermckenzie.com

processors specifically reflect their more limited role in dictating the manner and means of personal data processing.

- Offences under the Law can be committed by:
    - Egyptian companies operating in Egypt or overseas;
    - Foreign companies operating in Egypt; and
    - Foreign companies where the offence is punishable by law in the country where the perpetrator is based, and where it concerns a data subject resident in Egypt or a data subject who is a foreigner but who resides in Egypt.
- The Law introduces a breach reporting deadline equivalent to the GDPR. Specifically, data breaches must be notified to the Regulator (as defined below) by the controller or processor, as the case may be, within 72 hours.
- Foreign companies processing personal data in Egypt are obliged to appoint a representative in Egypt. Further details are to be published in the Regulation.
- All controllers and processors in Egypt must appoint a Data Protection Officer who is an Egyptian resident.
- The Law also imposes a licensing, permit and security accreditation framework for data processing, data control, dealing in sensitive data, electronic marketing, and cross-border transfer of data.
- Companies should monitor the publication of the Regulation, which will provide further detail on the key provisions under the Law such as its extraterritorial application.

In more detail

Scope of application

Article 1 of the Law solely applies to personal data that has been electronically processed, whether partially or entirely, hence data held exclusively in a physical format is not regulated. This is contrary to the position under the GDPR and data protection laws introduced in some other African countries.

Article 3 outlines a number of important exceptions to the Law, such as where the data is processed by a natural person for personal use, where it is used for informational purposes provided it is true and accurate and used only for that purpose or the personal data is held by the Central Bank of Egypt or any of the entities subject to its purview (with the exception of money transfer and exchange companies).

The offences under the Law apply extraterritorially. The penalties will apply if the offence under the Law is also penalised (in any form) in the foreign country in which the act occurred. The offenders caught are those who are Egyptian or foreign nationals in or outside of Egypt and the data subject relates to Egyptians or non-Egyptians residing in Egypt.

It remains to be seen to what extent the Regulation will clarify how the Law will be applied to foreign controllers and processors. In addition, we note that Article 3 could potentially result in a company being penalised twice if the data subject is an Egyptian who resides in a foreign country and the breach of the Law committed also triggers penalties under foreign law.

Processing conditions

Under Article 3 of the Law, many of the same core principles of EU data protection law are replicated such as that the processing must be lawful, transparent and that the personal data collected should be retained for no longer than is necessary to fulfil the intended purpose. The same is also true for the legal bases which can be relied by controllers to legitimately process personal data. These include consent of the data subject and where the processing is in the controller's legitimate interest (provided the latter does not contradict the basic rights and freedoms of the data subject).

Permission to process sensitive personal data is more stringent. Importantly, the definition of sensitive data under the Law includes children's data and will require the consent of their legal guardian. Consent is also required as a legal basis for direct marketing.

DPO appointment

Controllers and processors of personal data must appoint a Data Protection Officer (**DPO**) who will be the primary point of contact for the relevant company in all dealings with the Regulator. An official register will be maintained by the Regulator of all registered DPOs. Importantly, under the Law there are no exemptions to this obligation for small companies.

The Law specifies that the DPO is responsible for implementing the requirements of the Law and also sets out a range of additional duties in Article 9. The Law currently envisages that the DPO will be an employee of an Egyptian company, hence it appears at present that it will not be possible to outsource this function. The Regulation will hopefully clarify this point, and whether a global DPO or a group DPO can be appointed (i.e., to satisfy the obligations of multiple companies within a corporate group).

For data controllers outside of Egypt a local representative must be appointed as a point of contact for Egyptian data subjects and the Regulator.

Cross-border transfers

Article 14 of the Law stipulates that in order to transfer personal data out of Egypt, a company must obtain a license from the Regulator and should only transfer personal data to a country which affords the same level of protection to personal data as Egypt under the Law.

Article 15 sets out a number of exceptions to the Article 14 restriction, which are all contingent on first obtaining the express consent of the data subject.

Notification requirements

In the event of a security breach, unlike under the GDPR, both controllers and processors are obliged to report the incident to the Regulator within 72 hours. In the case of a breach which impacts national security, companies must report the incident to the Regulator and the National Security authorities immediately, including the Ministry of the Interior and the General Intelligence Directorate amongst others.

Companies must also be aware of the existing obligation to report any cyber-attacks to the National Telecommunication Regulatory Authority as part of the Anti-Cyber and Technology Crimes Law (available in Arabic here).

Data subject rights

Article 2 of the Law details a list of rights data subjects are granted in relation to their personal data, which include, amongst others, the right to revoke consent to processing, to object to processing, and to have their data rectified. However, interestingly exercise of these rights can be subject to payment of a fee of up to a maximum of 20,000 EGP (equivalent to approximately USD 1,250).

In contrast to the GDPR, as part of the transparency obligations, data controllers in Egypt do not have to disclose a privacy notice before processing personal data. However, they must maintain a register in accordance with Article 4 that describes the erasure mechanism, the retention period of such data, and so forth.

Regulator and sanctions

The enforcement of the Law will be led by the establishment of a new data protection regulator called the Personal Data Protection Centre (**Regulator**). Article 19 provides a comprehensive list of the Regulator's duties and competencies. In particular, it will be responsible for issuing licenses to companies in order to process or make cross-border transfers of data. The Regulator will have 90 days to consider an application for a license. The maximum fees for an application will be 2 million EGP (equivalent to approximately USD 125,000).

Failure to adhere to the Law may result in the Regulator imposing onerous criminal and financial penalties on both controllers and processors, depending on the circumstances. Directors and managers can also be held personally liable for regulatory breaches.

Some of the key offences and penalties include:

- Article 36 - Unlawful disclosure of personal data, which will result in a fine of between 100,000 - 1 million EGP (USD 6,300 to USD 63,000). The fines will be doubled if the disclosure is for a moral benefit at the expense of the data subject and will also result in imprisonment for a minimum of six months. If the unauthorised disclosure concerns sensitive data, the fines levied are between 500,000 - 5 million EGP (equivalent to approximately USD 31,000 and USD 315,000) and a minimum three months' imprisonment.

- Article 40 - Failure to appoint a DPO or failure by a DPO to carry out their duties will result in a fine between 200,000 - 2 million EGP (equivalent to approximately USD 12,500 and USD 125,000).

- Article 42 - Violation of cross-border transfer requirements will result in a fine between 500,000 - 5 million EGP (equivalent to approximately USD 31,000 and USD 315,000) and a minimum of three months' imprisonment.

- Article 42 - Violation of the electronic marketing rules will result in a fine not less than EGP 200,000 - 2 million EGP (equivalent to approximately USD 12,500 and USD 125,000).

Overall, the new Law marks a significant step towards strengthening Egyptian residents' rights of privacy and to creating a transparent and solid legal foundation to support the growth of the Egyptian technology sector and to drive Egypt's digital transformation forward. Domestic companies will have a lot of work to do and we recommend that they begin to consider now what steps they need to take to achieve compliance. While the grace period appears generous,

we are aware from our experience with preparing companies for the enforcement of the GDPR that the work required can be time consuming. For multi-national organisations that already abide by the GDPR, or similar privacy frameworks, the Law doesn't present many new concepts. However, the ease with which those companies can secure the required licenses or permits will be fundamental.

For further information, please feel free to contact one of the lawyers above or your usual Baker McKenzie contact.