

Egypt's new personal data protection law

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
- Riyadh

Ayman Nour - Partner, Head of Office - Egypt - Corporate Structuring / Corporate Services / Projects
a.nour@tamimi.com - Cairo



Egypt's new data protection law has been a long time coming. Media reports over the last year or two have resulted in ambiguity as to the status of the draft law.

We are pleased to advise that Egypt's Personal Data Protection Law was passed on 13 July 2020 and published on 15 July 2020. It will come into force on 14 October 2020, and the Executive Regulations are expected by 14 April 2021.

The Personal Data Protection Law introduces a variety of compliance requirements, as well as some significant criminal penalties. Corporate clients processing personal data in Egypt, or outside Egypt in respect of individuals in Egypt, should familiarise themselves with the requirements and ensure compliance as soon as possible.

The Personal Data Protection Law defines 'Personal Data' as any data related to an identified natural person, or to a natural person identifiable, directly or indirectly, by reference to any other data, such as name, voice, picture, identification number, online identifier, or any data that identifies psychological, health, economic, cultural or social identity. 'Sensitive Personal Data' is defined as Personal Data that discloses psychological, mental, physical or genetic health, biometric data, financial data, religious beliefs, political opinions or security situation; and Personal Data relating to children is deemed to be Sensitive Personal Data.

The Personal Data Protection Law prohibits the processing of personal data except with the consent of the data subject, or where otherwise permitted by law.

Data Subjects have various rights under the Personal Data Protection Law. These include the right to:

- know what personal data is being processed by whom, and to access the same;
- withdraw consent in respect of processing personal data;
- correct, modify, delete, add or update his or her personal data;
- limit processing of his or her personal data within a limited scope;
- be notified of any personal data breach involving his or her personal data.

With the exception of the right to be notified of a personal data breach, the Personal Data Protection Law

contemplates data controllers or data processors being able to charge data subjects a fee in respect of the exercise of these rights.

Subject to certain exceptions, the Personal Data Protection Law contains a general prohibition on the transfer of Personal Data to recipients located outside Egypt except with the permission of the (yet to be established) Egyptian data protection centre/authority ('Egyptian DPA') and where the level of protection provided is not less than that provided in Egypt pursuant to the Personal Data Protection Law. The Executive Regulations will specify the policies, standards, guidelines, and rules necessary for transferring Personal Data across borders.

The exceptions to the prohibition on transfers of Personal Data to places outside Egypt may be summarised as follows:

- explicit consent of the Data Subject to the proposed transfer;
- protecting the vital interests of the Data Subject;
- exercise of a legal right, or defence of a legal claim;
- for the performance of a contract, between the Data Controller and a third party, in favour of the Data Subject;
- exercising a special procedure relating to international judicial cooperation;
- in the performance of a legal obligation or to protect a legal interest; and
- pursuant to an international obligation to which Egypt is a party.

The Personal Data Protection Law contemplates circumstances where a Data Controller or Data Processor may, with the permission of the Egyptian DPA, allow other Data Controllers or Data Processors outside Egypt to have access to Personal Data. These include circumstances where the purposes for which they have access to the Personal Data is identical, where such access is in the legitimate interests of the Data Subjects, the Data Controllers or the Data Processors, and where the level of legal and technical protection to the subject Personal Data is not less than that to which the Personal Data would be subject in Egypt. Again, the Executive Regulations will specify the related policies, standards, guidelines, and rules necessary for transferring Personal Data across borders in this context.

The Egyptian DPA is responsible for enforcement of the requirements of the Personal Data Protection Law at an administrative level. Without prejudice to any criminal or civil liability that may apply, the Egyptian DPA may issue notices in respect of non-compliance, directing those responsible to address the instance of non-compliance within a specific period of time. If the issue is not addressed, the Egyptian DPA may impose administrative penalties, including suspension or withdrawal of licences or accreditations, publication of details of the non-compliance in the media, and making the relevant Data Controller or Data Processor subject, at their own expense, to technical supervision by the Egyptian DPA to ensure compliance with the requirements of the Personal Data Protection Law.

The Personal Data Protection Law also provides for a variety of criminal offences, with a range of penalties, including fines and imprisonment. These include:

- Collecting, processing, disclosing, providing access to, or circulating Personal Data, by any means, other than with the consent of the Data Subject, or as otherwise permitted by law (imprisonment for not less than one year, and a fine of between EGP 100,000 and EGP 1,000,000 (between about US\$6,300 and US\$63,000));
- Processing Personal Data other than in accordance with the Personal Data Protection Law (imprisonment for not less than three months, and/or a fine of between EGP 100,000 and EGP 1,000,000 (between about US\$6,300 and US\$63,000));
- Preventing a Data Subject from exercising rights granted pursuant to the Personal Data Protection Law (imprisonment for not less than three months, and/or a fine of between EGP 100,000 and EGP 1,000,000 (between about US\$6,300 and US\$63,000));
- Failure of a Data Controller or Data Processor to comply with obligations of the Data Controller,

obligations on the Data Processor and obligations to notify and report as specified in the Personal Data Protection Law (imprisonment for not less than six months, and/or a fine of between EGP 200,000 and EGP 2,000,000 (between about US\$12,600 and US\$126,000);

- Failure to appoint a Data Protection Officer, or to provide the same with essential requirements to perform duties (a fine of between EGP 200,000 and EGP 1,000,000 (between about US\$12,600 and US\$63,000);
- Failure of a Data Protection Officer to perform duties as specified in the Personal Data Protection Law (imprisonment for not less than six months, and/or a fine of between EGP 100,000 and EGP 1,000,000 (between about US\$6,300 and US\$63,000);
- Transferring Personal Data other than in accordance with the Personal Data Protection Law (imprisonment, and/or a fine of between EGP 300,000 and EGP 3,000,000 (between about US\$18,900 and US\$189,000);
- Failure to comply with digital marketing requirements pursuant to the Personal Data Protection Law (imprisonment for not less than three months, and/or a fine of between EGP 100,000 and EGP 1,000,000 (between about US\$6,300 and US\$63,000);

These are examples of some offences and penalties; others are set out in the Personal Data Protection Law. The penalties specified are without prejudice to any harsher penalties that may be provided for in any other law. Employees of corporate entities, as well as corporate entities themselves, may be responsible for the offences, depending on the circumstances of the offence.

While the Executive Regulations have yet to be issued, corporate clients processing personal data in Egypt, or outside Egypt in respect of individuals in Egypt, should start to familiarise themselves with the requirements of the new law, and start taking steps to be in a position to ensure compliance.

For further information, please contact [Nick O'Connell \(n.oconnell@tamimi.com\)](mailto:n.oconnell@tamimi.com) or [Ayman Nour \(a.nour@tamimi.com\)](mailto:a.nour@tamimi.com).