Cairo, Egypt | 22 July 2020

NEW LAW ALERT: PROTECTION OF PERSONAL DATA

Over the past couple of years Egypt has witnessed rapid legislative developments and a reformative wave in the spheres of cyberspace, information technology and regulation of internet activities. These developments are attempts to evolve the regulation of the online sphere, safeguard content available online, eliminate cybercrimes and provide protection for online users. Among this wave was the issuance of the cybercrimes law, which sets out regulatory framework for online activity on the cyberspace and outlaws activities that are considered cybercrimes and violation of privacy and a draft law on protection of personal data that was in the parliament's pipeline for the past year and a half.

The long anticipated law governing protection of personal data and privacy was promulgated and issued and will enter into force and become legally binding on 16 October 2020. The Data Protection law specifically focuses on safeguarding the personal data of individuals, which are being stored, processed or controlled electronically through online platforms.

Cornerstone of the New Law

The law sets rights to data subjects (i.e. individuals whose data is being electronically stored, processed or controlled) and sets obligations on controllers and processors of such personal data. It is applicable to personal data that belongs to Egyptians residing in Egypt and abroad, as well as foreigners residing in Egypt. The new law aims to regulate and monitor the usage of personal data of individuals and set the parameters for disclosure of such data, which is not permissible without the explicit consent of the data subject (i.e. to whom such personal data belongs).

The cornerstone of the new law is to obtain the explicit consent of data subjects prior to storing and processing their data, protect such data from damages and cyberattacks, non-disclosure of data and most importantly to provide data subjects with an opt-out option.

What are the Types of Data under the Law?

The new law categorizes personal data under two types:

- *Personal data*, which includes any data relating to an identified natural person or one who can be identified directly or indirectly by way of linking personal data to another such as: a name, a voice, a picture, an identification number, an online identifier, or any data which determines the psychological, physical, economical or cultural identity of that person.
- *Sensitive data*, which includes data relating to mental, physical or psychological health, genetic data, biometric data, financial data, religious beliefs, political views, criminal records, and children's data.

In certain cases the law does not provide protection of certain types of data, such as data required for criminal investigations or national census purposes.

What are the Main Obligations on Controllers and Processors?

Amongst the obligations imposed on Controllers are:

- Non-disclosure of data without explicit consent of the user (except to cases permissible under the law).

- To only collect data for specific purposes made known to the data subject.
- Assure that the collected personal data suffice for the purpose of its processing.
- Assure the non-availability of personal data unless authorized under the applicable laws.
- Take all technical necessary measures to safeguard the data, assure its non-disclosure or damage and protect it from any security breaches.
- Maintain ledgers to record data in a manner as outlined under the law.

While obligations imposed on Processors include:

- Process personal data legitimately and in a way that is compatible with the purpose for which it was collected.
- Not to retain data for a period longer than what is necessary for the purpose for which it was collected.
- Assure protection of data and its non-disclosure and safeguard all electronic devices used for processing data to assure its security from any breaches.
- Not to cause the data owner any harm or damages directly or indirectly.
- Keep a ledger to record all processing activities and information regarding such as outlined under the law.

How to Report Security Breaches?

The new law sets obligations on data controllers and processors to report any security breaches that occur to their server or data base within a course of 72 hours and sets out the procedures and guidelines for reporting. The controllers and processers are also under the obligation to inform the data subject of any breach of their data.

Watershed for Direct Marketing

The new law is a turning point for the direct marketing environment in Egypt, which has been unregulated for too long. It sets restrictions on marketeers and outlines the framework for direct marketing. Marketeers carrying out direct marketing must obtain a license or permit from the personal data protection center in order to carry out such activities. It also sets obligations on marketeers to obtain the consent of persons receiving the direct marketing material beforehand, a duty not to share the emails to whom it sends direct marketing material with any third parties and keep record of the data subject's consent for three (3) years from the last date of communication. It also gives data subjects the right of an opt-out option.

Transfer of Personal Data Cross-borders

It also sets out the guidelines for the transfer of data by controllers and processors to other controllers or processors outside of Egypt. This is particularly significant to companies that have their databases or servers set outside of Egypt, while retaining data of Egyptian or foreigners residing in Egypt. It imposes on controllers and processors the obligation to obtain license or approval for transferring of data cross-borders with few exceptions.

How does the Data Protection Law Impact your Business?

Any businesses that store, process or control data electronically especially businesses operating in online platforms will be subject to the application of the law. Businesses must revisit their privacy policies and apply for the necessary licenses and approvals and they must also appoint a data protection officer. The law grants a grace period for compliance with its provisions within one year from date of issuance of the executive regulations of the law. The executive regulations have not been issued yet, however, it is anticipated that they will be issued within six months.

Repercussions of Non-compliance

The non-compliance with the provisions of the law result in criminal liability on not only the data protection officer and the de facto manager, but also a criminal liability on the corporate entity.

For any questions or inquiries, please feel free to contact:

Omar Bassiouny
Founding Partner and Head of Corporate and M&A
omar.bassiouny@matoukbassiouny.com

Rana Shafik
Associate
rana.shafik@matoukbassiouny.com

CAIRO OFFICE
12 Mohamed Ali Genah
Garden City, Cairo, Egypt
T +(202) 2796 2042
F +(202) 2795 4221

www.matoukbassiouny.com