A Step in the Right Direction: Draft Data Protection Law in Egypt

by Ayman Nour - a.nour@tamimi.com - Cairo
Youssef Sallam - y.sallam@tamimi.com - Cairo, Egypt

June – July 2019

The Egyptian Cabinet of Ministers has recently approved a draft data protection law in Egypt (the 'Draft Law') which is currently being reviewed by Parliament. While the Draft Law may witness changes in Parliament, it is likely that many of its core tenets will not change. The Draft Law attempts to mimic the EU's General Data Protection Regulation ('GDPR') in more ways than one. The reason for that is twofold: the first reason being that the GDPR offers a good regulatory framework to apply; while the second reason is that it is much easier to interact with the EU on a technological level when data protection is comparable to that of the EU. One of the many ways in which the Draft Law is similar to the GDPR is in the former's definition of personal data.

Definitions

The Draft Law defines personal data as *"any data relating to an identifiable natural person, or is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, voice, picture, an identification number, an online identifier or to one or more factors specific to the physical, mental, economic, cultural or social identity of that natural person."* ('Personal Data') This definition is taken almost verbatim from the GDPR.

The Draft Law further identifies sensitive personal data, similarly to the GDPR, as *"data which reveal the mental health, physical health, genetic health, biometric data, financial data, religious beliefs, political opinions, security status relating to the natural person. In all cases, data relating to children are considered sensitive personal data."* ('Sensitive Personal Data').

Scope of Application

The Draft Law applies to partially or fully electronically processed data with any holder, controller, and processer of data related to all natural Egyptian persons as well as non-Egyptians residing in Egypt.

The crimes committed under the Draft Law can also apply to non-Egyptians if the act committed is punishable where it occurred and relates to the data of Egyptians or non-Egyptian residents.

The Draft Law does not apply to the following:

1. Personal Data held by natural persons for others and that is processed for personal use;
2. Personal Data processed for official statistics or in the application of a legal provision;
3. Personal Data processed for media purposes, provided the data is correct, accurate and not used for other purposes;
4. Personal Data related to judicial reports, investigations and claims; and

5. Personal Data in the possession of national security entities (defined as the Presidency, the Ministry of Defence, the Ministry of Interior, General Intelligence, and the Administrative Control Authority).

The Personal Data Protection Centre (as defined below) must, upon the request of the national security entities, notify the controller or processer to amend, delete, not show, make available, or circulate Personal Data for a defined period of time. Controllers and processers are obliged to execute the request.

The Draft Law will become effective three months from the date of publication and relevant parties will be required to reconcile their status within one year from the issuance of the executive regulations, which should be issued within six months from the date of promulgation of the Draft Law.

Personal Data Protection Centre

The Draft Law establishes a personal data protection centre which is tasked with regulating data protection, issuing licences, creating regulations and mechanisms to ensure data protection, and receiving complaints (‘Personal Data Protection Centre’ or ’Centre’)

Licences and Permits

The Centre is tasked with issuing licences or permits for: controllers, processers, consultants, direct marketing activities, organisations, unions, or clubs; controlling and processing sensitive Personal Data; visual surveillance of public spaces as well as cross-border transfers.

It is worth noting that an entity may hold more than one licence or permit.

Rights of Data Subjects

The Draft Law grants a set of rights to the data subject, who is any natural person whose Personal Data is processed (‘Data Subject’), in order to protect their data from controllers and processors.

Most importantly, Personal Data may not be collected, processed or disclosed, without the explicit and rescindable consent of the Data Subject.

The Data Subject also has the right to know, inspect, access, correct, and determine the degree of processing of their Personal Data possessed by any holder, controller or processer. Though the aforementioned rights can be exercised in exchange for a fee not exceeding EGP 20,000, the right to know of any breach of Personal Data is free of charge. Such access requests must be met or rejected within six working days, provided that, in the case of rejection, the decision indicates the reasons for rejection.

In order to collect and process data, the Personal Data must be

- used for legitimate, specific and public purposes;
- correct and accurate; and
- held only for the period of time required to fulfil its specified purpose.

Complaints

The Data Subject is also entitled to lodge a complaint to the Personal Data Protection Centre against the controller of the processer for a breach of data protection and for the denial of access to Personal Data. Such complaints must be decided upon within 30 working days and the controller or processer of data must comply with the Centre's decision within seven working days.

Obligations of the Controller and Processer

The Draft Law imposes a number of obligations on the controller and processer of Personal Data in order to protect the Data Subject and ensure compliance with the Draft Law.

The controller of Personal Data is obliged to:

- obtain Personal Data upon the explicit consent of the Data Subject;
- ensure that the Personal Data is accurate and sufficient for its intended purpose;
- design and implement methods and standards for processing Personal Data, unless the controller has delegated a processer;
- ensure that the processing of Personal Data is in line with the purpose of Personal Data collection;
- ensure access to Data Subjects;
- take all necessary security and protection measures and implement relevant standards to ensure that Personal Data is not breached or tampered with;
- delete Personal Data after its stated objective is met and, in the case of legitimately retaining Personal Data, ensure that the Personal Data is kept in a way that cannot identify the Data Subject;
- correct any mistake in Personal Data upon knowledge or notification;
- hold a Personal Data log including the Personal Data categories, those allowed access and their capacity, time periods, restrictions, scope, deletion and amendment mechanisms, and any information related to cross-border transfers as well as technical and regulatory procedures to maintain the security of the data; and
- obtain the necessary licence or permit from the Centre to control the Personal Data.

The processer of Personal Data is obliged to:

- comply with the Draft Law's requirements (and its executive regulations) for processing along with the written instructions from the Centre and the controller;
- ensure that the objectives of the Personal Data processing are legitimate and are not in contravention with public order or morality;
- remain within the parameters and time limits of stated objectives of the processing;
- delete the Personal Data after the lapse of the processing period;
- ensure access to Data Subjects;
- not engage in any process in contravention of the controller's objectives unless for statistical or educational purposes that are not for profit, while not infringing on the sanctity of private life;
- secure the processing of data and the equipment used;
- not directly or indirectly inflict harm on the Data Subjects;
- hold a process operation log that includes the processing categories, time periods, restrictions, scope, deletion and amendment mechanisms, and any information related to cross border transfers as well as technical and regulatory procedures to maintain the security of processing operations;
- ensure the capabilities to prove compliance with the Draft Law; and
- obtain the necessary licence or permit from the Centre to control the Personal Data.

Processing Conditions

Processing Personal Data is considered legitimate in any of the following cases:

- to obtain the consent of the Data Subject;
- where processing is necessary and required, in compliance with a contractual obligation, or to enter into a contract with a Data Subject;
- in compliance with a legal obligation (court order or investigation);
- to allow the controller to fulfil its obligations, insofar as it does not contravene with the Data Subject's rights.

Reporting Requirements

The controller and processer are required to notify the Centre of any breach of Personal Data within 24 hours from the time of the breach. They are also required to submit a detailed report of the breach within 72 hours. The Centre, in turn, shall immediately notify national security entities. The controller and/or processer is also required to notify the Data Subject of the breach within 10 working days from notifying the Centre.

Data Protection Officer

According to the Draft Law, the controller and/or processer of Personal Data is required to appoint a data protection officer who shall be placed in charge of complying with the Draft Law, conducting regular inspections, receiving and responding to requests from Data Subjects and the Centre.

Cross Border Transfers

The Draft Law also stipulates that transferring or sharing Personal Data abroad shall only occur by obtaining a permit from Centre, provided that the state to which the Personal Data is being transferred has equal or greater data protection regulations. The processer or controller may provide access to Personal Data to another controller or processer provided the objectives are similar or in case of a legitimate benefit to the controller, processer or Data Subject.

Provided explicit consent from the Data Subject is obtained, Personal Data can be transferred to a state with lesser degrees of data protection in the following cases:

- protecting the life of the Data Subject and to provide medical care;
- in order to prove, claim, or defend a right before the judiciary;
- in fulfilment of a contract for the benefit of the Data Subject;
- making monetary transfers; and
- in order to fulfil a treaty of which Egypt is a member.

Direct Marketing

The Draft Law sets out conditions for direct marketing to Data Subjects which includes obtaining a licence, prior consent from the Data Subject, stating the sender, and creating a clear opt-out

mechanism

Sanctions

Sanctions for violating any of the provisions of the Draft Law range from administrative penalties such as warnings and suspension or revocation of licences to fines not exceeding EGP 2 million and/or jail sentences.
However, the Draft Law does permit reconciliation or settlements outside of court with the Data Subjects or the Centre.

Conclusion

The Draft Law helps regulate an area of law that had thus far remained woefully unregulated by the government. Provisions governing data protection have been scattered across several laws and regulations with no clear or definitive protection. In order to keep in line with global data protection trends as well as the internal need for a regulatory framework, it became clear that a comprehensive data protection law was necessary. Most importantly, the GDPR has created a framework to which we aspire.

Al Tamimi & Company's Corporate Structuring team regularly advises on Data Protection issues in Egypt. For further information please contact Ayman Nour (a.nour@tamimi.com) or Mohamed Khodeir (m.khodeir@tamimi.com).