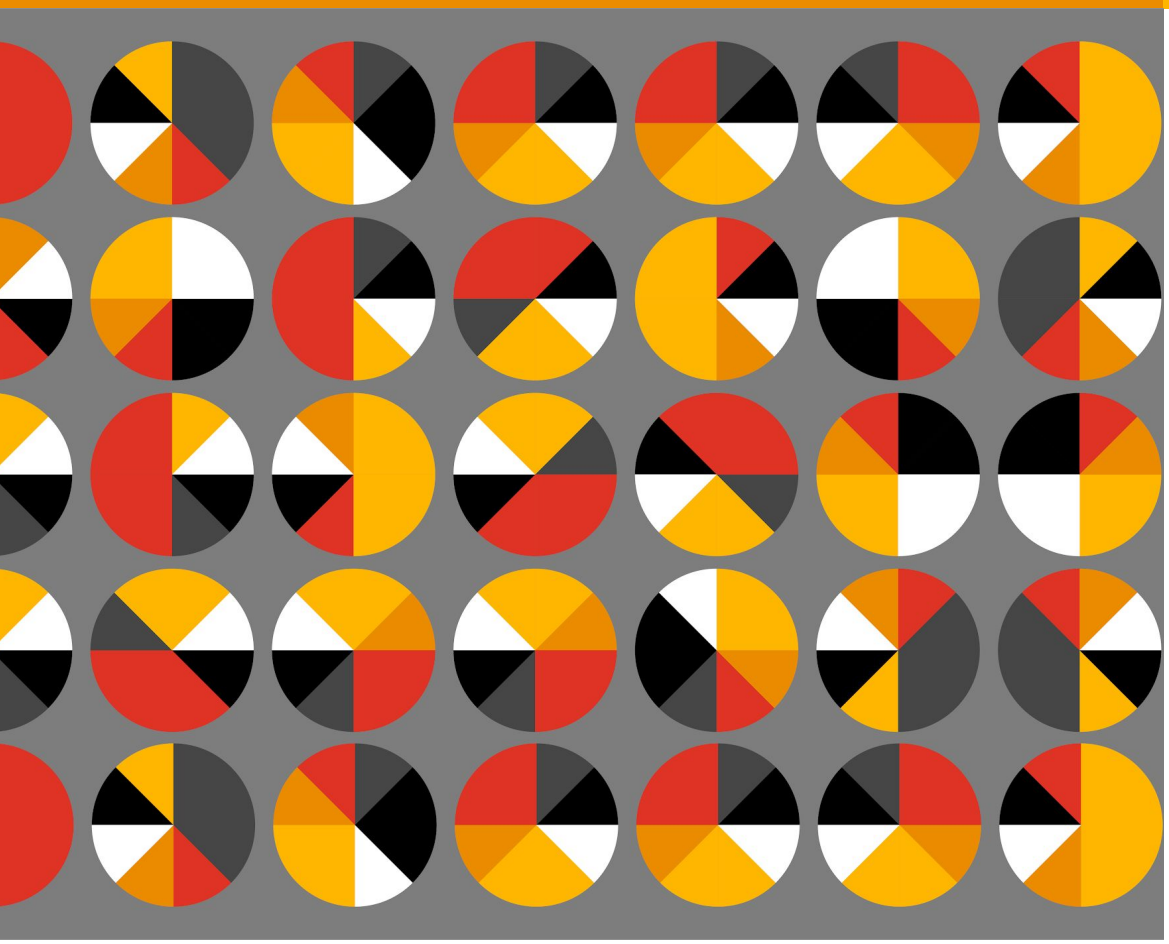
Egypt: A New Data Privacy Law

November 2019



Insights
Tax and Legal Services
PwC Middle East

pwc

In brief

On 3 November 2019, the Egyptian House of Representatives was reported to have approved, in principle, the draft of Egypt's first data protection law (Draft Law). The law is expected to be officially published by the end of 2019 and will come into effect three months from that date, with additional implementing regulations required to be issued within a further 6 months. Organisations in Egypt are then expected to have 12 months to develop and implement their data protection compliance programs in order to ensure that they comply with the law.

The Draft Law may require many companies operating in Egypt to rethink their personal data processing activities. The law will introduce strict requirements businesses must adhere to in order to be permitted to process people's personal data and businesses will need to familiarise themselves with these obligations quickly. Investment in appropriate processes, measures and protocols to safeguard personal data are also likely to be required.

In detail

Background

Whilst modelled to a large extent on the EU General Data Protection Regulation (GDPR), the Draft Law diverges in several key areas, including exempting the Central Bank of Egypt (CBE) and all entities (including banks) subject to its supervision, from the scope of the law. Other differences in the Draft Law include no restrictions on the processing of special category personal data (e.g. health, racial, religious data) or criminal convictions data and a different regime governing cross-border data transfers. In addition, the Draft Law does not recognise the legal basis of processing personal data where this is necessary to enable the data controller to pursue some legitimate interest. Both areas feature prominently in the GDPR. Finally, the GDPR places the principle of transparency (i.e. requiring that any information addressed to individuals be concise, easily accessible, easy to understand, and presented in clear and plain language) at its very core. The Draft Law does not contain such emphasis.

Notwithstanding this however, the Draft Law does draw heavily from its European counterpart because:

1. the GDPR is seen as the leading data protection regulatory framework globally (thus making it good commercial and competitive sense to mimic many of its provisions); and
2. technological interfacing can be easier when the data protection laws in the respective jurisdictions are comparable.

Application

The Draft Law will apply to personal data of Egyptian citizens and non-citizen residents in Egypt processed, in whole or in part, by electronic means by a controller or processor. In addition, it would appear that the Draft Law may also apply to non-Egyptians not residing in Egypt where an offence is committed against and/or relating to the personal data of Egyptians or non-Egyptian residents.

The following categories of personal data are also stated to fall outside the scope of the Draft Law:

- personal data held by natural persons for others and that is processed for personal use;
- personal data processed for official statistics or in the application of a legal provision;
- personal data processed for media purposes, provided the data is correct, accurate and not used for other purposes;

- personal data related to judicial reports, investigations and claims; and
- personal data in the possession of the Presidency, the Ministry of Defence, the Ministry of Interior, General Intelligence, and the Administrative Control Authority.

Regulator

The Draft Law will establish the "Personal Data Protection Centre" (PDPC) to regulate data protection, enforce compliance with the law, create further implementing regulations and mechanisms to ensure data protection, and receive and investigate complaints. In addition, the PDPC is tasked with issuing licences or permits authorising certain restricted types of personal data processing. Organisations wishing to carry out certain processing activities must obtain a licence from the PDPC prior to doing so, including in order to:

- process sensitive personal data;
- carry out visual (e.g. CCTV) surveillance of public spaces in Egypt; and
- transfer personal data outside Egypt.

The PDPC is required, when requested to do so by an Egyptian national security authority, to notify any controller or processor to amend, delete, withhold, make available, or circulate personal data for a defined period. Controllers and processors are obliged to comply with any such request.

Personal Data

The Draft Law replicates, practically verbatim, the definition of "personal data" contained in the GDPR, stating that personal data is "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."

The Draft Law similarly takes the definition of special category personal data predominantly from the GDPR, defining it as any "data which reveals 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."

Data Protection Principles

Like the GDPR, the Draft Law incorporates and follows several internationally accepted fundamental principles of data protection law, practice and procedure. These principles will govern the practices of organisations in Egypt that collect, process and store personal data. Specifically, this principles-based approach to personal data processing will require organisations to:

- only collect and process personal data for specified, legitimate and public purposes and not process it in a manner inconsistent with those purposes;
- ensure all personal data processed is correct, sufficient and accurate and update/correct data where necessary;
- not retain personal data once the purpose(s) of the processing have been achieved; and
- take all necessary security and protection measures and implement relevant standards to guard against unauthorised access or use of personal data.

Lawful Purpose

The Draft Law states that controllers must have a valid lawful basis in order to process personal data. The law provides four available lawful bases which may be relied on to process personal data with no one single basis being 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual:

- the individual has given consent to the processing of their personal data for one or more specific purposes;
- the processing is necessary and required by a contractual obligation, or to enter into a contract with the individual;
- the processing is necessary in order to enable the controller to comply with a legal obligation imposed on it (court order or investigation); and
- to allow the controller to fulfil its obligations under the Draft Law, provided it does not offend against the individual's rights.

Controller Obligations

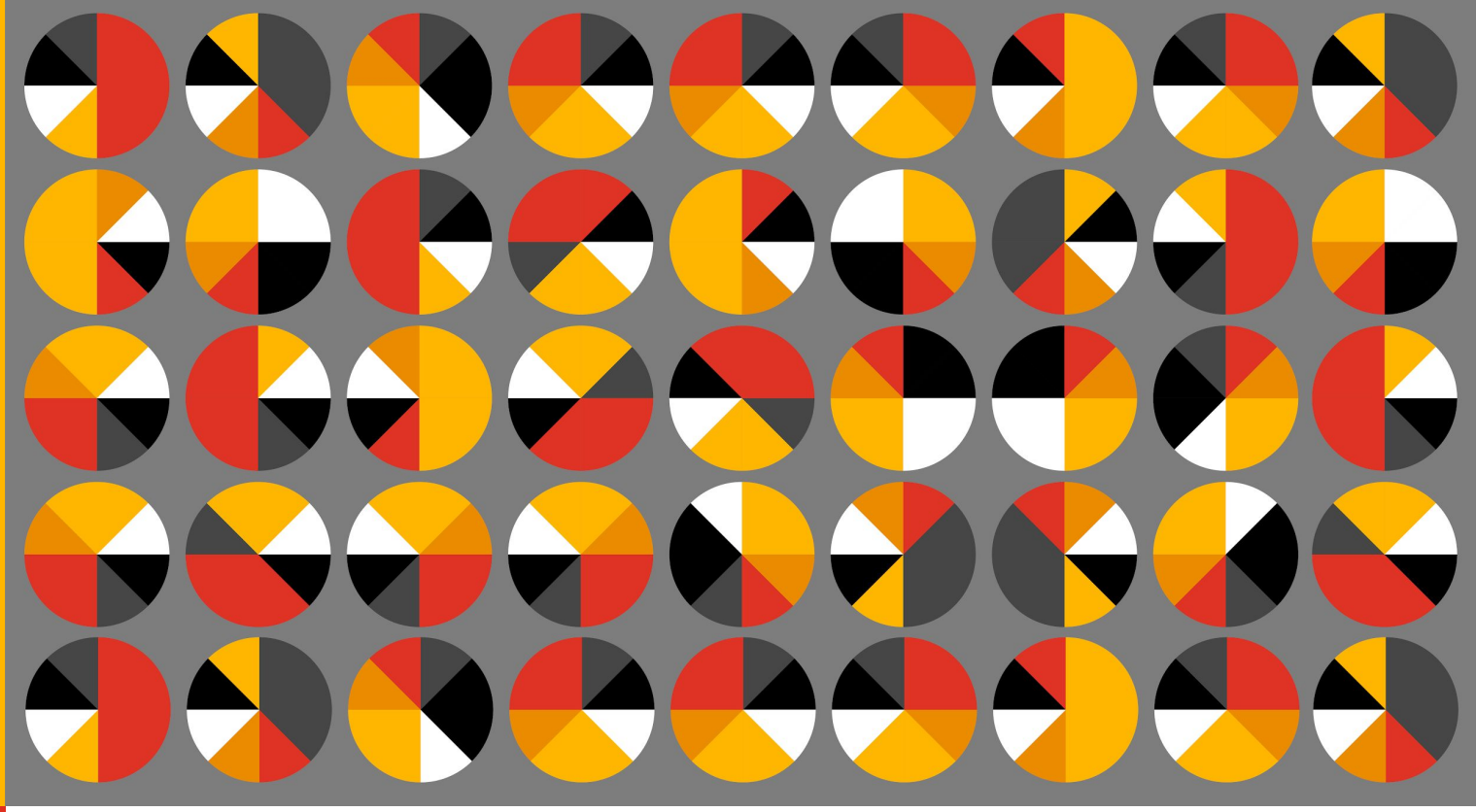
In addition to the core data protection principles, the Draft Law imposes a number of explicit obligations on controllers of personal data, requiring them to:

- design and implement methods and standards for processing personal data, unless the controller has appointed a processor;
- give effect to individual access requests;
- if there is a legitimate reason for retaining personal data after the stated purpose(s) for collecting it has been achieved, ensure that the personal data is kept in a way that cannot identify the individual;
- compile and maintain a "Personal Data Log", detailing the categories of personal data, the identity of those who have access to the data, relevant retention periods, any restrictions imposed on processing data, procedures for deleting and/or updating data, technical and organisational measures used to secure the data and any cross-border transfers of data; and
- obtain any necessary licence(s) or permit(s) from the PDPC to process personal data.

Processor Obligations

Processors equally have a number of explicit obligations imposed on them by the Draft Law, including:

- complying with any written instruction in relation to the processing of personal data from the PDPC and/or the controller;
- ensuring that the objectives of any personal data processing are legitimate and do not offend against public order or morality;
- delete or return personal data to the controller once the purposes of the processing have been achieved;
- not carrying out any processing outside the controller's specific instructions unless for statistical or not-for-profit educational purposes;
- compile and maintain a "Personal Data Log", detailing the categories of personal data, the identity of those who have access to the data, relevant retention periods, any restrictions imposed on processing data, procedures for deleting and/or updating data, technical and organisational measures used to secure the data and any cross-border transfers of data;
- be able to demonstrate compliance with the Draft Law; and
- obtain any necessary licence(s) or permit(s) from the PDPC to process personal data.



Individual Rights

As with most modern data protection laws that take a principles-based approach, the Draft Law grants individuals a number of rights in relation to their personal data. Central to these rights is that no controller or processor may collect, disclose or process an individual's personal data without their explicit, rescindable consent.

Individual rights under data protection law are designed to enable individuals to exercise control over if and how their personal data may be processed. In this regard, individuals have the following key rights under the Draft Law:

- the right to be informed whether a particular controller or processor processes their personal data;
- the right to request that the organisation provide them with access to/a copy of their personal data that is being processed;
- the right to have that personal data corrected where it is inaccurate or out-of-date; and
- the right to determine the extent to which the organisation may (continue to) process their personal data.

With the exception of the "right to be informed", organisations may charge individuals a fee for honouring any individual request not exceeding EGP20,000. All access requests must be either met or rejected within 6 working days and, where it is rejected, the reasons for such rejection must be communicated to the individual.

In addition to the access rights, individuals are also entitled to lodge complaints with the PDPC against controllers and/or processors for breaches of the Draft Law, including for failing to give effect to their access rights. Once a complaint is received, the PDPC must render a decision on it within 30 days and any order made by it must be complied with by the relevant controller/processor within 7 working days.

Data Breach Reporting

Controllers and processors are required to notify the PDPC of any breach of personal data within 24 hours of the breach. They are also required to follow up with a detailed report of the breach within 72 hours. Individuals must also be informed of the breach within 10 working days of notifying the PDPC.

The breach notification requirements under the Draft Law are markedly different than the GDPR. Under the latter regime:

- the obligation to notify breaches to the regulator rests with the controller alone but processors are required to notify the controller of any incidents without undue delay;
- breaches must be notified to the data protection authority only if there is a risk to the rights of the individual and individuals only need to be notified, without undue delay, if these risks are high; and
- controllers have 72 hours to notify a data breach the data protection supervisory authority.

Data Protection Officer

The Draft Law requires that both controllers and processors appoint a data protection officer to be responsible for:

- monitoring the organisation's compliance with the law;
- conducting regular inspections;
- receiving and responding to requests from individuals; and
- acting as a point of contact with the PDPC on issues relating to compliance.

Cross Border Transfers

The Draft Law recognises that transfers of personal data to other countries can give rise to risks for the data, the individual and the transferring organisation. Therefore, before any controller or processor can transfer personal data outside Egypt, they must obtain a permit from the PDPC. It appears that such permits will only be granted if the jurisdiction to which the data is to be transferred has a data protection framework that will provide at least equal or greater protection for personal data than the Draft Law. Interestingly, the Draft Law also provides that a controller or processor may provide a third party with access to the personal data they hold if the objectives of the third party are similar or if there is some legitimate benefit to be derived from such access by the controller, processor or individual.

Personal data may be transferred to countries that have lesser degrees of data protection than Egypt provided that:

- the explicit consent of the individual has been obtained; and
- the transfer is necessary for the purposes of:
    - protecting the life of the individual and to provide medical care;
    - proving, claiming, or defending a right before the judiciary;
    - fulfilling a contractual obligation for the benefit of the individual;
    - making monetary transfers; and
    - fulfilling a treaty of which Egypt is a member.

Direct Marketing

The Draft Law also addresses the issue of direct marketing, stating that before engaging in this activity, organisations must:

- obtain a licence from the PDPC; and
- obtain the prior consent of individuals.

In addition, the content of all direct marketing messages must clearly state the identity of the organisation sending the message and provide a clear opt-out mechanism.

Sanctions

The financial remedies and sanctions available to the PDPC and/or aggrieved individuals in Egypt are comparatively low under the Draft Law when compared to, for example, the GDPR. Under the Draft Law fines may be imposed up to a maximum of EGP2 million (approx. US$124,000) versus the higher of approx. US$22.5 million or 4% of global turnover under the GDPR). Notwithstanding this however, the possibility of imprisonment for breaches of the Draft Law arguably still gives the Draft Law real 'teeth'. Interestingly, the Draft Law also specifically allows for reconciliations or settlements outside of court with the aggrieved individual(s) and/or the PDPC.

The PDPC is also empowered to issue warnings for instances of non-compliance and to suspend or revoke any license or permit previously issued to the offending controller or processor.

The takeaway

Data privacy is quickly becoming a matter for the C-Suite agenda in MENA, and indeed globally. Organisations everywhere are being impacted both operationally and financially by the wave of new data privacy laws and those operating in Egypt will be no different. Egypt's Draft Law seeks to steer the country toward established international best practices and principles and to ensure consistency and familiarity for Egyptian businesses who fall within the scope of the GDPR and/or operate internationally where expectations over data privacy are high. The Draft Law should also work to enhance the attractiveness of Egypt to foreign investors by providing a clear framework for processing personal data.

In preparation, companies operating in Egypt will need to determine if their business activities bring them within the scope of the law. If they do, the next step is to determine what sort of personal data is being collected, from who, and what purposes it is being used for. Businesses in particular will need to identify all the third parties with whom they share their personal data, e.g. payroll providers, cloud service providers etc. They must also familiarise themselves with the circumstances in which licences/permits from the PDPC must be obtained in order to engage in certain data processing activities. All of this will require business to invest in appropriate processes, measures and protocols to safeguard their personal data.

www.pwc.com/me

Let's talk

For a deeper discussion of how this issue might affect your business, please contact:

Matt White
Partner, Head of Digital Trust
+971 56 113 4205
matt.white@pwc.com

Darren Harris
Head of Legal Services
+971 56 418 9768
darren.harris@pwc.com

Phil Mennie
Partner, Digital Trust
+971 56 369 7736
phil.mennie@pwc.com

Richard Chudzynski
Legal Data Privacy Leader
+971 56 417 6591
richard.chudzynski@pwc.com