Preparing for UAE's new PDL

Whilst the data protection regulations have yet to be published the new law has sufficient detail to allow organisations to gear up. Saleem Adam and Sapna Desai set out their responses to the ten FAQs on the new UAE Data Protection Law.

1 What is the new law called and why is it so important?

The Federal Decree-Law No.45/2021 on the Protection of Personal Data is referred to as the new Data Protection law of the UAE (the "PDL"). It did not replace any other law and is the first comprehensive law to govern the use of personal data in mainland UAE. Organisations are required to keep data secure, be aware of data breach obligations and abide by various provisions regarding the safeguarding of data.

In fact, the PDL also broadly mirrors the provisions and principles of the EU General Data Protection Regulation (the "GDPR") - the GDPR being generally deemed as the "gold standard" for data privacy standards and practices globally. The PDL should therefore not simply be regarded as a new law in mainland UAE but more crucially as something which seeks to reflect international global standards around the protection and use of personal data.

2 To whom does the PDL apply?

Broadly speaking, if you process personal data of UAE residents then you will have to adhere to the PDL even if you are based abroad. Certainly, the PDL is likely to be welcomed by businesses who are used to abiding by the existing data protection rules in other jurisdictions to ensure consistency across the group. However, organisations that are not used to compliance with data protections laws, like the GDPR, are expected to find the obligations of the PDL challenging.

3 How long do I still have to comply?

If you are still playing catch up then you still have time to comply. In fact, organisations have a period of six months from when the executive regulations, which supplement the PDL, ("Executive Regulations") are published to achieve compliance with the PDL. If you need to fine-tune your operations to comply with the PDL, there is still time.

4 How do the Executive Regulations, which are yet to be issued, affect the PDL?

It is not yet clear exactly when the Executive Regulations will be published although this had originally been envisaged as being within the first six months of the law coming into effect. It is anticipated that

the Executive Regulations will clarify a variety of points covered in the PDL, including setting out specific cases where personal data can be processed without specific consent (in addition to those already set out under the PDL), the procedures and timeframes for reporting a personal data breach, details surrounding administrative penalties for breaches of the PDL and Executive Regulations as well as the controls and requirements for cross-border transfers of personal data. Our recommendation is to avoid waiting for the Executive Regulations to be published because there is sufficient detail in the PDL to allow organisations to adjust operations now.

5 What kind of information does the PDL apply to?

The PDL applies to "personal data", meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. Personal identifiers include a name, voice, picture, identification number, an online identifier, geographic location, or one or more special features that express the physical, physiological, economic, cultural or social identity of a person.

Crucially, organisations need to take extra care when processing "sensitive personal data". Like the GDPR, this includes (amongst others) personal information about someone's racial origin, political, philosophical, or religious beliefs, biometric data or any data related to a person's health or physical, psychological, mental condition. As drafted, the PDL shall not apply to the processing of government data, or processing by government authorities that control or process personal data, free zones or those organisations that have their own sector laws.

6 What responsibilities do businesses have under the PDL?

Under the PDL, organisations have to meet seven data protection principles (as further described in Question 7 below) whenever they process personal data - including ensuring that their use of personal data is lawful, fair and transparent and that collection is for a specific and clear purpose. Those who do collect it are obliged to protect it from misuse and exploitation.

If a data breach does occur, for example, if information gets lost or stolen, then organisations are required under the PDL to report certain types of breaches to the UAE Data Office, and/or the individual in question. The exact scope and period within which such a report must be made is anticipated to be set out in the Executive Regulations. The Executive Regulations may also set out certain additional data protection principles to the seven already provided under the PDL.

7 What rules should businesses follow to ensure compliance?

The PDL's Article 5 states that personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected only for specific and clear purposes;
3. sufficient for and limited to the purpose for which it is processed;
4. accurate, correct and kept up to date;
5. erased or corrected if incorrect personal data is kept;
6. kept securely and protected from any breach or unauthorised processing; and
7. kept only so long as is necessary for the purpose for which it is processed (personal data may only be kept beyond this if it is anonymised).

In addition to the above, there must be a "legal basis" before personal data can be lawfully processed. Consent of the relevant individual (which in itself must be clear, specific, informed and unambiguous meaning that in practice, a pre-ticked consent box would not suffice as valid consent) is set out in the PDL as being the default legal basis however there are various other legal bases that an organisation may rely on as an alternative to consent (to the extent it is appropriate for it to do so) such as to where:

1. the processing is necessary to protect the public interest or the interest of the individual;
2. the processing is necessary to perform a contract to which the individual is a party;
3. the processing is necessary to fulfil obligations and exercise legal rights in the field of employment or social security; and
4. the personal data has become available and known to the public by an act of the individual.

“As drafted, the PDL shall not apply to the processing of government data, or processing by government authorities that control or process personal data, free zones or those organisations that have their own sector laws.”

8 What are an individual's fundamental rights under the PDL?

Given that the PDL is the first law in the field of data protection to be introduced in mainland UAE, individuals are for the first time awarded with a number of new rights, as follows:

1. **The right to obtain information** - individuals have a right to be informed about the use of their personal data including what type of personal data an organisation collects about them and processes, the purpose for such collection, with whom the personal data will be shared with, how long the personal data will be kept for, protection measures for cross-border transfers of personal data and the relevant procedures for correcting or erasing their data and to be taken in the event of a breach of their personal data.
2. **The right of rectification** - individuals are entitled to request the correction or completion of their personal data if it is inaccurate or incomplete.
3. **The right to erasure** - this refers to an individual's right to request that their personal data is erased on the basis that they no longer consent to the processing of their personal data, the personal data is no longer required for the purpose for which it was collected or if they object to the processing of their data.
4. **The right to restrict processing** - this refers to an individual's right to block or suppress the processing of their personal data where they object to the accuracy of their personal data or argue that the processing violates the agreed purposes or legislation in force.
5. **The right to request a personal data transfer** - individuals are entitled to request, under certain circumstances, for the transfer of their personal data from one data controller to another, should they choose to do so.
6. **The right to stop processing** - in certain circumstances, individuals are entitled to object to their personal data being processed if a company uses personal data for direct marketing, for conducting statistical surveys (unless necessary in the public interest) or if processing violates any of the controls set out in the PDL.
7. **Rights related to automated processing** – individuals have the right to object to decisions issued with respect to automated processing that has legal or serious consequences for the individuals.

9 Does every business need to appoint a Data Protection Officer (DPO)?

It is not compulsory for businesses to appoint a DPO however it may nonetheless be good practice for certain businesses to do so. The requirement depends upon a number of factors and each business will need to carry out its own assessment to determine whether they do in fact need to appoint one. For instance, a DPO is required if the processing involves large amount of sensitive personal data. It is also expected that the Executive Regulations will set out further details on the appointment of a DPO.

10 What are the penalties for breaches?

The Federal Cabinet is yet to confirm the acts that would constitute a violation of the PDL and Executive Regulations together with the administrative penalties to be imposed, although the specific timelines as to when such decision is to be issued is not yet clear.

Text by:
1. SALEEM ADAM, *resident managing partner, Trowers & Hamlins, Abu Dhabi*
2. SAPNA DESAI, *associate, Trowers & Hamlins, Abu Dhabi*