UAE's New Federal Data Protection Law

The UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection was issued on 20 September 2021 ("Law").

The Law will become effective on 02 January 2022. Executive regulations are due to be issued within 6 months of the date of issuance of the Law (i.e. by 20 March 2022). UAE companies will then have 6 months from the issuance of those executive regulations to comply with the Law (although that period can be extended by the Cabinet). As with many UAE laws, the executive regulations will contain a great deal of additional detail on the provisions of the Law and assist UAE companies in understanding their compliance requirements under the Law.

The Law looks to align UAE's Federal law with global "best practice" data protection principles. For those familiar with such principles, much of the Law will be familiar with key transparency and accountability concepts included. The Law introduces data subject rights, data breach requirements, data protection impact assessments, data transfer requirements and notification and record keeping requirements.

In tandem with the Law, UAE Federal Decree-Law No.44 of 2021 Creation of the UAE Data Office was also issued on 20 September 2021. The UAE Data Office ("Data Office") will act as the data protection regulatory authority, operationalizing the Law's requirements.

Key Aspects

Who does the Law apply to? The Law applies to both controllers and processors. A controller is a person or entity that determines the method and criteria for processing personal data and the purpose for the processing. The processor processes the personal data on behalf of, under the direction of and in accordance with the instructions of the controller.

Personal data covers any data relating to a natural person or relating to a natural person who can be identified directly or indirectly by linking data. It covers, without limitation, name, voice, picture, identification number, electronic identifier, geographical location or one or more of the natural person's physical, physiological, economic, cultural or social characteristics and includes sensitive personal data.

Sensitive personal data covers data that directly or indirectly reveals the family or ethnic origin of a natural person, political or philosophical opinions or religious beliefs, criminal record, biometric data and any data relating to a natural person's health.

The Law applies to the processing of all personal data by controllers and processors located in the UAE whether or not the personal data processing relates to data subjects in the UAE or abroad. It covers the personal data of data subjects residing or working in the UAE.

It also applies to controllers and processors located outside the UAE who are processing personal data of UAE data subjects – an extra-territorial element similar to GDPR.

There is a materiality threshold in the Law in relation to the processing of personal data with the Data Office having the ability to exempt UAE companies that do not process large volumes of personal data. This will be set out in the executive regulations.

Who does the Law not apply to? The Law does not apply to government data, government authorities that control or process personal data, or personal data processed by the security and judicial authorities. It does seem as government companies will, though, be covered by the Law. It does not cover personal health

data and information, or personal banking and credit data and information where there is separate legislation covering such personal data and information. The Law also does not apply to UAE free zones, such as the Dubai International Financial Centre and the Abu Dhabi Global Market that have their own data protection laws. Finally, the Law does not apply to the use of personal data for personal purposes by a data subject.

What are the Law's key personal data principles? The Law talks in terms of personal data processing "controls". These include: processing in a fair, transparent and lawful manner; collecting personal data only for a specific and clear purpose; only processing such personal data as it necessary based on the specific purpose (or for purposes similar or close to the specific purpose); keeping personal data accurate, correcting or deleting inaccurate personal data; keeping personal data secure; only keeping personal data for as long as required based on the specific purpose and then either deleting or anonymizing it. All these principles are consistent with those adopted by global data protection laws, like the GDPR.

What are the lawful bases for processing personal data under the Law? Personal data can only be processed with the consent of the data subject except in certain limited circumstances. These prescribed circumstances include: processing where necessary to implement a contract with a data subject or to conclude, amend or terminate any such contract; where the data subject has made the personal data public; to protect the interests of the data subject; where processing is necessary for claiming legal rights or as part of judicial or security procedures; where processing is necessary for certain medical purposes or matters of public health (in accordance with relevant legislation); for archival purposes or for scientific, historical and statistical studies (in accordance with relevant legislation); and/or for a controller or data subject meeting obligations and exercising employment/social protection rights.

One lawful basis for processing that has not been included is where processing is necessary for the purposes of the legitimate interests pursued by the controller (or by a third party), which is a common basis provided in global data protection laws.

Further legal bases for processing may be specified by executive regulations.

How should consent to processing personal data be managed? Controllers will need to be able to establish the consent of the data subject where consent is used as the lawful basis for processing the data subject's personal data. The consent should be clear, simple, unambiguous and easily accessible, it should be made through a statement or clear affirmative action and can be writing or provided electronically (e.g. a tick the box). The consent wording should include the right for the data subject to withdraw from the consent and such withdrawal should be simple. Data subjects can withdraw consent at any time. Such withdrawal shall not affect the legality and lawfulness of the Processing made based on the Consent given prior to the withdrawal.

What are the key controller obligations? Controllers have a number of key obligations. These include taking appropriate technical and organizational measures to protect personal data (and manage automatic processing to ensure it is limited to its intended purpose); maintaining a "special record" of personal data (and making it available to the Data Office on request along with any other information the Data Office requires); and ensuring processors provide sufficient guarantees and implement technical and organizational measures necessary to meet the requirements of the Law.

What are the key processor obligations? Processors must only process personal data in accordance with the controller's instructions and on the basis of any agreements signed between the controller and the processor. Processors must apply appropriate technical and organizational measures to protect personal data and secure the processing process (including any devices used for the processing). Processors are also required to maintain a special record of the personal data processed on behalf of a controller. . Processors must also ensure that processing is in accordance to the specified purpose and specified processing period, and notify the Controller if the processing exceeds this period. The Law looks to mandate that where

multiple processors are undertaking processing activities on behalf of a controller, an agreement clearly detailing and governing that processing will be required.

Is there detail on the technical and organizational measures to be taken by controllers and processors? The Law sets out that both controllers and processors must develop such procedures and take such measures as required in accordance with best international standards and practices, and commensurate to the risk and cost involved with the processing, to ensure an appropriate level of information security. The Law includes a list of such measures, including encryption 'pseudonymization' , and "anonymization" (which are defined terms in the Law). These measures need to be tested and evaluated.

What is the process for reporting a personal data breach? Controllers must, on becoming aware of any personal data breach that would "*prejudice the privacy, confidentiality and security of a data subject's personal data*" inform the Data Office of the breach and any investigation conducted into the breach". The Law sets out details to be included in any notification and the executive regulations will add further details, including any reporting period. The controller must also notify the data subject of the breach and there is no higher threshold (e.g. high risk) for any such data subject notification than that which is set for notifying the Data Office. Processors must inform the controller of any breach as soon as they become aware of it.

Will a data protection officer need to be appointed? It is only mandatory for a controller or the processor to appoint a data protection officer (DPO) in respect of certain processing of personal data. The Law requires both the controller and the processor to appoint a sufficiently skilled and knowledgeable DPO where the processing creates a high risk to the privacy of the personal data through either the adoption of new technologies or the volume of personal data processed. A DPO will also be required where processing involves the assessment of sensitive personal data as part of profiling or automated processing or where large volumes of sensitive personal data are processed. The executive regulations will provide more specifics to assist in determining whether "high risk" processing is taking place and a DPO is, as a result, required. A DPO can be located outside the UAE. The Law envisages the DPO acting as the link between the controller and processor and the Data Office and sets out criteria for how controllers and processors should support the DPO.

Does the Law include data subject access rights? Yes. The Law sets out a list of information that a data subject can request from a controller. The controller may only reject a data subject's request in limited circumstances. For example, where the request is for information not covered under the Law; or where the request is overly repetitive, conflicts with judicial procedures or investigations; could adversely affect the controller's information security efforts or otherwise affects the privacy and confidentiality of others' personal data. The information needs to be provided without charge. The Law does not set out a timeline for a controller to respond to a data subject access request, although this may be covered in the executive regulations.

What other data subject rights are there? Similar to other global data protection laws, data subjects have various rights: the right to data portability; right to the rectification or erasure of personal data (i.e. the right to be forgotten); the right to restrict personal data processing; the right to object to personal data processing (e.g. for marketing purposes); and the right to object to decisions resulting from automated processing (including profiling) that have legal consequences or seriously affect the data subject. Data subjects can file complaints with the Data Office if they have reason to believe there has been a breach of the Law in relation to the processing of their personal data. The Law places certain limitations on the exercise of several of these data subject rights. Controllers must put in place clear and simple means by which the data subject can contact the controller and exercise their rights.

Are there any data subject notification requirements under the new Law? Yes. A controller must, before processing a data subject's personal data, provide the data subject with the purposes for the personal data processing, any third parties that the personal data will be shared with and the protection measures put in place to cover any cross-border data transfers. Whilst not as prescriptive as other data protection laws in

relation to how data processing activities are documented and communicated to data subjects, this would seem to place a requirement on controllers to put some form of data protection notice or policy in place. .

What do the data protection impact assessments cover? Controllers are required to assess any proposed processing operations where the use of technologies could pose a high risk to the privacy of personal data. Assessments will be required where processing covers automated processing, including profiling, or involves a large volume of sensitive personal data. The DPO role will be important for the management of these assessments. The Data Office will be releasing details of those processing operations that will not require assessments.

What the rules are around cross border personal data transfers? The Law allows for the transfer of personal data to countries approved by the Data Office as having an "adequate level of protection". These cover countries that either have "special legislation" in place for the protection of personal data or where the specific country has acceded to bilateral or multilateral agreements relating to the protection of personal data. While it is not expressly stated in the Law to be the case, we would expect the executive regulations to include details of the approved countries. For countries not approved by the Data Office as having an adequate level of protection, the Law provides various options to enable the transfer of personal data. These include transferring personal data under a contract that applies the requirements of the Law (similar, we assume, to the standard contract clauses used under other global data protection laws); securing the data subject's express consent to such transfer (where such consent does not conflict with public and security interests of the UAE); if the transfer is necessary for the execution of a contract between the controller and the data subject (or as part of a contract between the controller and a third party that achieves the interests of a data subject); if the transfer is necessary for international judicial cooperation, or if the transfer is necessary to protect the public interest . More details are expected in the executive regulations.

What is the Law's penalty regime? Administrative penalties can be imposed as part of a decision by the Council of Ministers in response to a breach of the Law or the executive regulations and based on a proposal from the Data Office's Director General. The Law does not specify the range of potential administrative penalties. Data subjects can file a complaint with the Data Office if they have reason to believe that the Law has been breached by a controller or processor.

What is the Data Office? The Data Office will be established under a separate statute (Federal Decree-Law No. 44 of 2021) which was issued contemporaneously with the Law. The Data Office aims to ensure the fullest protection of Personal Data and is affiliated with the Cabinet. The Data Office is responsible for a range of tasks which include:

- preparing legislation and policies relating to data protection;
- proposing and approving mechanisms for data subject complaints and compensation;
- proposing standards for the monitoring of the data protection legislation;
- issuing guidance for the full implementation of data protection legislation.
- imposing administrative penalties.

Courtesy to:

https://www.tamimi.com/news/uaes-new-federal-data-protection-law/