Baker McKenzie Habib Al Mulla.

Client Alert
December 2021

UAE: Personal Data Protection Law coming into force on 2 January 2022

In brief

On 27 November 2021, the UAE published the long awaited UAE Personal Data Protection Law, Federal Law 45 of 2021 on Personal Data Protection (the "**Law**"). The development signifies a landmark in the evolution of the UAE's regulatory framework and lays the foundation for the modernization of the economy and digitization of the country's growth sectors.

The Emirates Data Office (the "**Data Office**") will act as the new data regulator and will be established by virtue of Federal Law 44 of 2021. Amongst other responsibilities, the Data Office will be responsible for enforcing the Law and for issuing supporting legislation and guidance.

The Law will come into force on 2 January 2022 with its Executive Regulations, which will expand on key topics, to be published within six months of the Law entering into effect (currently 28 May 2022). Controllers and processors will have six months from the date the Executive Regulations are issued to achieve compliance with the Law, although the Data Office has the ability to extend this period if necessary.

In this alert, we set out 10 key aspects of the Law with a view to helping businesses to understand its impact and to prepare for its entry into force.

Key takeaways

- The Law will be effective from 2 January 2022 but companies will have until November 2022 at a minimum to adapt their operations to achieve compliance with the Law.
- The Law borrows heavily from the EU General Data Protection Regulation ("**GDPR**"), reflecting many of its key concepts including the data protection principles (i.e., the core principles that underpin all personal data processing such as a need to ensure that processing is fair, transparent and lawful; that the personal data processed is adequate and relevant for the purpose; and that the personal data is kept secure and protected against unauthorized processing using appropriate organizational and technical measures).
- The Law has extra-territorial application and imposes obligations on both controllers and processors (as those terms are commonly understood under EU data protection law) although the obligations imposed directly on processors are more limited.
- The default position under the Law is that consent of the data subject must be obtained to conduct processing, subject to certain exemptions, such as where the processing is necessary to perform a contract to which the data subject is a party or where the processing is necessary to comply with the controller's legal obligations.
- Under the Law, there is no legal basis for processing personal data that is equivalent to the legitimate interests legal basis contained in Article 6(1)(f) of the GDPR. Companies which currently rely on this legal basis or an equivalent legal basis under foreign laws will need to legitimize their processing in reliance on an alternative legal basis under the Law.
- The Law introduces a requirement for controllers and processors to appoint a Personal Data Protection Officer ("**DPO**") in similar scenarios to those set out in the GDPR, including where the processing presents a high-level of risk to the confidentiality and privacy of the data subject as a result of the adoption of new technologies or the volume of personal data under processing.

- The Law contains a personal data transfer mechanism that varies depending on whether the receiving country affords or does not afford an adequate degree of protection to personal data. Further requirements for transfers made to non-adequate jurisdictions will be set out in the Executive Regulations.
- The Law imposes a duty on controllers to report details of any breach that compromises the privacy, confidentiality or security of data subjects' personal data to the Data Office as well as to the affected data subjects in certain circumstances.
- The Law does not prescribe any penalties for breach of its requirements but provides that the UAE Cabinet will issue a decision specifying the acts that constitute a breach of the Law and the associated administrative penalties based on a proposal of the Director General of the Data Office.

Companies should monitor for the publication of the Executive Regulations, which will provide further detail on certain requirements under the Law, including the timescales for reporting data breaches and the requirements for transferring personal data to non-adequate jurisdictions.

In the meantime, given that the majority of the Law's requirements are entirely new, we recommend that companies take full advantage of the grace period to assess the Law's impact and to reflect the requirements in their compliance programs.

In more detail

1. Scope and Application

The requirements of the Law apply to:

a) data subjects who reside in or who work in the UAE;
b) every controller and processor located in the UAE, irrespective of whether their processing of personal data takes place inside or outside of the UAE;
c) controllers and processors located outside the UAE that process the personal data of UAE data subjects; and
d) all automated digital processing of personal data.

Importantly, the obligations under the Law do not apply to:

a) government data nor government entities that control or process Personal Data;
b) personal financial or credit data or health data, in each case to the extent that it is already governed by other UAE legislation (i.e., the Health Data Law); or
c) companies and establishments in the free zones in the UAE that are subject to their own personal data-related legislation; including for example the DIFC and the ADGM.

2. Personal Data

For the purposes of the law, personal data is defined as any data relating to an identifiable natural person, or related to a natural personal that can be identified directly or indirectly by linking the data, through the use of identifiers. A data subject is a natural person who is the subject of personal data.

Included within the definition are the sub categories of data that of a more sensitive nature ("**Sensitive Data**") that include data that, directly or indirectly reveal a natural person's:

- family;
- ethnic origin;
- political or philosophical opinions;
- religious beliefs;
- criminal record;
- biometric data; or

© 2021 Baker & McKenzie Habib Al Mulla

- any data relating to a person's health, including their physical, psychological, mental, genetic or sexual condition, including information related to the provision of health care services that reveal the condition of their health.

3. Lawful Bases for Processing Personal Data

The default position under the Law is that a data subject's consent is required to process personal data unless an exemption applies. The definition of consent is broadly similar to the same concept contained in the GDPR, namely it must be specific, clear and unambiguous and must be indicated through a clear positive act. Consent is also revocable, which may well create barriers when attempting to rely on it as a primary means of legitimizing processing.

Amongst other reasons, the exemptions to the general rule described above include where the processing is necessary:

- to perform a contract to which the data subject is a party or to take measures at the request of the data subject with the aim of concluding, amending or terminating a contract
- to implement specific obligations in other laws applicable where the controller is located;
- to initiate or defend any claim or legal proceedings or when the processing is necessary for judicial or security measures;
- for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis or the provision of health, social care or treatment; or
- needed by the controller or Data Subject for the purposes of performing its obligations and exercising its legally established rights in the area of employment, social security, or the laws concerning social protection to the extent permitted by such laws.

Importantly the Law does not allow for processing to be carried out in the pursuit of the controller's legitimate interests nor the legitimate interests of a third party, which marks a sharp departure from the GDPR and reflects the approach adopted in the Saudi Personal Data Protection Law published in September 2021. Additional legitimate bases for processing may be introduced in the Executive Regulations.

4. Controller Obligations

A controller is defined broadly as an establishment or natural person who determines the means, manner and standards for processing personal data and the purpose of the processing, whether alone or jointly with others.

The Law imposes general obligations on controllers, which are generally aligned with those applicable under the GDPR including that the controller must:

a) provide certain information to the data subject prior to conducting processing;

b) put in place appropriate technical and organizational measures and procedures to protect the personal data in accordance with the applicable law;

c) maintain a record of processing that is available for inspection by the Data Office on request;

d) only appoint processors who can provide sufficient guarantees regarding the implementation of technical and organizational measures to ensure the processing satisfies the requirements and restrictions set out in the Law, the Executive Regulations and associated resolutions;

e) implement processes and procedures to give effect to the data subject's rights under the Law; and

f) appoint a data protection officer where required to do so under the Law.

A processor (defined as any company or establishment that processes personal data under the supervision and on the instructions of a controller) is obliged to comply with many of the same obligations as a controller, as well as certain obligations that are specific to their role such as where there is more than one processor, putting in place a written contract that determines the respective roles of the processors and outlines their respective responsibilities.

5. Personal Data Protection Officer Appointment

The Law requires controllers and processors to appoint a DPO where they satisfy one of the following threshold tests:

© 2021 Baker & McKenzie Habib Al Mulla

a) the processing presents a high-level of risk to the confidentiality and privacy of the data subject as a result of the adoption of new technologies or the volume of data under processing;

b) the processing includes a systematic and comprehensive assessment of Sensitive Data including profiling and automated processing; or

c) a significant volume of Sensitive Data is to be processed.

If a Personal Data Protection Officer is appointed they can either be an employee of the controller or processor or a person authorized by them to fulfil this role. Importantly, the appointed DPO can reside within or outside the UAE. Accordingly, multinational companies will have the option of appointing their existing group DPO for this purpose.

6. Data Subject Rights

The Law affords data subjects a number of rights that can be exercised in respect of their personal data, including to restrict or prevent its processing. Importantly, data subjects have been afforded a right to obtain certain information on request, free of charge, such as details of the purposes of processing, the measures that have been put in place in respect of cross-border transfers and the decisions made using automated processing.

In addition, they will have the right to ask for their Personal Data to be corrected and deleted in certain circumstances such as where they have withdrawn their consent to processing or the personal data is no longer required for the specified purpose.

Data subjects also have the right to receive a copy of their personal data in a machine readable format and can request for it to be transferred to another controller (if technically feasible). Notably, this right is addressed under the heading of 'data portability' and appears to be distinct from the concept of a general right of access. However, there is nothing in the Law that would prevent the right being exercised regardless of the circumstances.

The Law attempts to strike a balance between honouring the rights of data subjects and allowing controllers to decline requests in certain circumstances, for example where compliance with it may infringe on another data subject's rights or where the request is excessively repetitive.

7. Cross Border Personal Data Transfers

Personal data can be transferred outside the UAE where the transfer is being made to a jurisdiction that has adopted personal data protection legislation, provided the legislation in question reflects the most important provisions, measures, controls, conditions and rules for protecting the privacy and confidentiality of personal data, as well as honouring the data subject rights afforded by the Law and provisions relating to the enforcement of the relevant requirements by a regulatory or judicial authority.

In addition, transfers may occur to countries with whom the UAE has signed a multi-lateral or bilateral agreement for the protection of personal data. We expect the Data Office to publish a list of countries which will be treated as adequate for this purpose.

For transfers to non-adequate jurisdictions, the controller or processors can rely on one of the following security measures or derogations, amongst others, which are set out as legally equivalent options:

- a contract is put in place that obliges the data importer to implement the provisions, measures, controls and required contained in the Law;
- on obtaining the express consent of the data subject in a manner that does not conflict with the UAE's public interests or security interests;
- if the transfer is necessary to exercise or defend rights before judicial authorities; or
- the transfer is essential for the implementation of a contract between the data subject and controller, or third party in the data subject's interest.

The Executive Regulations are intended to set out further guidance on the controls and requirements that will apply when relying on the various options for legitimising transfers to non-adequate jurisdictions.

8. Data Protection Impact Assessments

© 2021 Baker & McKenzie Habib Al Mulla

Controllers are obliged to conduct a data processing impact assessment ("**DPIA**") in respect of processing activities that would pose a high risk to the privacy and confidentiality to a data subject's personal data. Unlike the GDPR, the Law does not require a DPIA to be conducted in respect of personal data processing in respect of the systematic monitoring of a publicly accessible area on a large scale.

Under the Law the Data Office has confirmed its intention to publish on its website a list of the types of processing operation that *do not* require a DPIA to be conducted.

9. Personal Data Breach Reporting

In the event of a data breach controllers are obliged to notify the Data Office (within the time period specified in the Executive Regulations) if the breach prejudices the privacy, confidentiality or security of data subjects. The controller is obliged to share the following documents with the Data Office upon notification:

- details of the breach and the potential consequences;
- the name of their appointed DPO (if any); and
- a description of any mitigations and corrective procedures undertaken to remedy the breach or its effects.

The processor must inform the controller *immediately* of a breach so that they can inform the relevant parties within the stipulated timeframes.

10. Complaints to the Data Office

Data subjects have the right to file a complaint with the Data Office if they believe their personal data has been processed by either the controller or processor in breach of the Law or if they believe that a provision of the Law has been broken. The Executive Regulations will provide further detail on the corresponding processes.

To speak to us in relation to the UAE Personal Data Protection Law or any data and technology related matters, please feel free to contact Kellie Blyth.

For future updates, you can visit and subscribe to our Middle East Insights blog: me-insights.bakermckenzie.com/

© 2021 Baker & McKenzie Habib Al Mulla

Contact Us

Kellie Blyth
Counsel
Dubai
kellie.blyth
@bakermckenzie.com

© 2021 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.