Baker McKenzie.

Client Alert
June 2020

New DIFC Data Protection Law – what you need to know and how to prepare

His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai has enacted a new DIFC Data Protection Law (**New DIFC Law**), which replaces the DIFC Data Protection Law of 2007 (as amended) (**2007 DP Law**).

The New DIFC Law reflects many of the requirements of the EU's General Data Protection Regulation (**GDPR**) seen by many as the 'gold standard' for data protection compliance. The New DIFC Law will predominantly apply to businesses with operations in the Dubai International Financial Centre (**DIFC**), an economic zone located in the Emirate of Dubai.

The new law will come into force on 1 July 2020. However, organisations will be given until 1 October 2020 to achieve compliance to allow for the impact of the COVID-19 pandemic on business operations. This gives organisations just a few months to make any changes required to bring their compliance frameworks into line with the new law.

Organisations with EU operations or who are otherwise subject to the GDPR are likely to be familiar with many of the New DIFC Law's concepts, and may already be in a good position to comply with the new law by adapting or re-purposing existing GDPR based policies and procedures.

From our previous experience in preparing for the GDPR coming into force, we recommend that organisations begin planning now. In particular, organisations should prioritise fact gathering and other time intensive tasks such as contract remediation.

Importantly, there are some key differences between the GDPR and New DIFC Law, which organisations should be aware of. We have summarised the key obligations under the New DIFC Law, as well as some of the differences to the GDPR, in our analysis.

1. Who does the New DIFC Law apply to?

The New DIFC Law applies to:

1. processing of Personal Data by Controllers or Processors incorporated in the DIFC, regardless of whether the processing takes place in the DIFC; and
2. Controllers or Processors, that process Personal Data in the DIFC (i.e. where the means or personnel used to conduct the Processing are physically located in the DIFC) as a part of stable arrangements (other than on an occasional basis), regardless of their place of incorporation.

Therefore, although, the New DIFC Law does not have extra territorial scope in the same way as the GDPR, it will capture Personal Data processing activities that take place outside of the DIFC, which are conducted by a company incorporated in the DIFC as well as Personal Data processing operations carried out by non-DIFC organisations using people or systems in the DIFC.

2. Data Protection Principles

As with the GDPR, the New DIFC Law sets out a series of data protection principles that organisations must comply with, which include (amongst others) familiar concepts such as lawfulness, fairness and transparency and privacy by design and default.

The New DIFC Law imposes an express obligation on Controllers and Processors to establish a compliance program to demonstrate compliance with the New DIFC Law. The complexity and level of detail in the program will depend in part on the scale and resources of the organisation in question as well as the risks the processing poses to data subjects. However, the program must demonstrate that the New DIFC Law's core principles are embedded within the organisation.

3. Data Protection Impact Assessments

Similar to the GDPR, the New DIFC Law requires a data protection impact assessment (or **DPIA**) to be conducted in certain circumstances, specifically where the organisation is conducting “High Risk Processing Activities”. The threshold that triggers this requirement under the New DIFC Law, as well as the required content of the DPIA are similar to the requirements under the GDPR, but are not identical.

Organisations will need to create (or review and update) a DPIA template and procedure to ensure DPIAs are conducted where necessary, and consult with the DIFC Data Protection Commissioner where required by the New DIFC Law.

4. Data Protection Officer (DPO)

The New DIFC Law requires Controllers and Processors to appoint a DPO if they carry out High Risk Processing Activities on a systematic or regular basis or if required to do so by the Commissioner.

If a Controller or Processor is not required to appoint a DPO, the organisation must clearly allocate responsibility within its organisation for oversight and compliance with its data protection obligations under the New DIFC Law (or any other applicable data protection law).

Organisations subject to the New DIFC Law will need to assess whether they are required to appoint a DPO under the New DIFC Law noting that the threshold is similar but not identical to the threshold under the GDPR.

The DPO must reside in the UAE unless the DPO is employed within the organisation's group and performs a similar function for the group on an international basis.

An important difference between the New DIFC Law and the GDPR, is that DPOs are required to conduct an annual assessment which reports on the Controller's processing activities and whether it intends to perform any "High Risk Processing Activities" in the following year.

5. Breach Notification Obligations

Similar to the GDPR, the New DIFC Law requires Controllers to notify the Commissioner in relation to Personal Data breaches, although the threshold under the New DIFC Law for when a notification is required is not identical to the GDPR requirement. In addition, the New DIFC Law only requires notification to the Commissioner "as soon as practicable in the circumstances", and does not impose a 72 hour time limit as is the case under the GDPR. Notably, there is also a requirement to notify breaches to data subjects in certain circumstances.

6. Record of Processing

Similar to the requirement under Article of 30 of the GDPR, organisations will need to understand what Personal Data they hold, why they are using it, as well as other key information required to be documented within a record of processing. This is likely to be one of the most time consuming tasks for organisations to complete and it should be prioritised. Organisations are required to review and maintain this record of processing on an ongoing basis.

7. Fair Processing Notices

Controllers are required to provide data subjects with fair processing notices. Although the content of such notices will be similar to those required to be provided under the GDPR, they will need to be tailored for compliance with the New DIFC Law, in particular to reflect one of the revised legal bases for processing. We note however that the legal bases set out in the New DIFC Law offer an additional degree of flexibility when compared with those included in the GDPR.

If a Controller intends to process Personal Data in a way which will restrict or prevent the data subject from exercising their rights to rectification, erasure or objection to processing, the Controller is required to provide a clear and explicit explanation of the anticipated impact to the data subject and must be satisfied that the data subject understands the extent of such restrictions. This is a key difference compared to the GDPR.

8. Data Subject Rights

Data subjects have similar rights under the New DIFC Law to those set out in the GDPR, including the right to withdraw consent, access their data or seek rectification or erasure of their data (amongst various others). However, organisations have additional flexibility compared to the GDPR in relation to certain data subject rights such as the right to object to processing, automated individual decision making and data rectification or erasure. Importantly, under the New DIFC Law a Controller is prohibited from discriminating against a data subject for exercising their statutory rights.

Organisations will need to ensure that they have a policy and procedure in place in order to respond to and appropriately handle data subject requests within the time periods stipulated. If organisations wish to leverage existing GDPR data subject rights policies, these will need to be reviewed and updated to reflect the nuances and differences between the GDPR and New DIFC Law.

9. Legal Basis for Processing

Organisations processing Personal Data will need to ensure they have a valid legal basis under the New DIFC Law for each processing operation they conduct, including for special categories of Personal Data. This assessment should be documented in order to demonstrate compliance with the New DIFC Law.

The legal bases for processing under the New DIFC Law are similar in many respects to those available under the GDPR, although the New DIFC Law provides additional flexibility, in particular with respect to the legal basis for processing special categories of Personal Data.

Importantly, the standard for consent under the New DIFC Law has been revised so that it reflects certain aspects of the GDPR; namely, it must be freely given and demonstrated by a clear affirmative act that shows an unambiguous indication of consent. Accordingly, if an organisation is relying on consent to conduct processing under the 2007 Law the consent will need to be refreshed to satisfy the new standard for validity.

10. Contracts with Processors

As with the GDPR, Controllers are required under the New DIFC Law to ensure certain mandatory obligations are included in agreements with Processors processing Personal Data on their behalf. This marks a significant change to the 2007 Law.

Although the list of mandatory terms is very similar to the GDPR, the audit rights required to be included in the agreement must extend to allowing the Commissioner to audit/inspect the Processor. Importantly, under the New DIFC Law, both the Controller and the Processor will be in breach of the law if they commence mutually agreed processing without having such a written contract in place.

Organisations should review and update existing contracts, as well as ensuring any new contracts include appropriate data processing terms. From our experience gained preparing for the GDPR coming into force, this contract remediation exercise can take a significant amount of time and must be commenced without delay.

11. International Data Transfer Restrictions

The New DIFC Law contains similar international data transfer restrictions to the GDPR, which will apply in respect of all transfers of Personal Data outside of the DIFC including to the UAE. Under the new law, organisations will no longer have the option to apply to the Commissioner for permission to make cross-border data transfers, and such transfers will only be permitted where there is an adequate level of protection in place to protect the Personal Data, or where one of the derogations set out in the New DIFC Law applies (for example, explicit consent or performance of a contract) and appropriate safeguards are in place.

Organisations will need to map their data flows to understand where Personal Data is being transferred to, whether inside or outside of their corporate group, and ensure that adequate safeguards are put in place, including where necessary standard contractual clauses.

12. Joint Controllers

Similar to the GDPR, where Controllers jointly determine the means and purposes of processing, they will be deemed to be "Joint Controllers". Under the New DIFC Law, there must be a legally binding written agreement (not an "arrangement" as is the case under the GDPR), which sets out their respective responsibilities, including the process for how data subject rights can be exercised and who is responsible for delivering fair processing notices to data subjects. The written agreement (or a summary of it) must also be made available to data subjects.

13. Enforcement

It is well documented that breaches of the GDPR can give rise to significant administrative fines of up to €10m or €20m or 2% or 4% of an organisations' total annual worldwide turnover for the preceding financial year, depending on the provision of the law that has been breached.

By contrast, the New DIFC Law does not stipulate a maximum cap on fines and gives the Commissioner discretion to impose a general fine in an amount the Commissioner considers appropriate and proportionate taking into account the seriousness of the breach and risk of actual harm to data subjects.

The Commissioner can also impose administrate fines in relation to contraventions of particular obligations under the New DIFC Law which are set out in Schedule 2 and which range from US$20,000 US$100,000.

14. Default Privacy Preferences

If a Controller offers online services via a platform, the New DIFC Law requires that the default privacy preferences on the platform are set to ensure that no more than the minimum amount of Personal Data is collected, which is necessary to deliver or receive the service.

15. Notification of Processing Operations

As was the case under the 2007 Law, Controllers and Processors are required to register with the Commissioner by filing a notification of processing operations. This notification must be kept up to date on an ongoing basis.

This notification and fee payment obligation applies to both Controllers and Processors, and it will be necessary to ensure these are made to the Commissioner and maintained on an ongoing basis.

Next Steps

Organisations in the DIFC should move swiftly to review their current data processing practices and to identify where their existing data protection policies and procedures will need to be updated to reflect the requirements of the New DIFC Law. Even where the organisation can leverage existing data protection policies and procedures prepared for GDPR compliance within their wider group, these will need to be reviewed and tailored to reflect the differences under the New DIFC Law.

Baker McKenzie's Data Protection team has far-reaching experience and in depth insight in relation to regional and international data protection compliance issues, including providing operational guidance and advice in relation to data protection and associated laws applicable in the DIFC,

ADGM, UAE and under the GDPR.

If you would like to get in touch with our team to discuss the changes to the New DIFC Law, please feel free to contact one of the lawyers below or your usual Baker McKenzie contact.

Contacts

Kellie Blyth
Head of Data and Technology
Dubai
Kellie.Blyth@bakermckenzie.com

Benjamin Slinn
Senior Associate
Data and Technology
London
Benjamin.Slinn@bakermckenzie.com