Client Alert

July 2020

New Dubai International Financial Centre Data Protection Law Comes Into Effect

On 1 July 2020, the Dubai International Financial Centre (DIFC) Data Protection Law No. 5 of 2020 comes into effect (New DP Law). Due to the current pandemic, a three-month grace period, running until 1 October 2020, has been provided for companies to comply. The New DP Law replaces DIFC Law No. 1 of 2007.

The release of the New DP Law is, in part, an effort to ensure that the DIFC, a financial hub for the Middle East, Africa and South Asia, meets the standard of data protection required to receive an "adequacy" finding from the European Commission and the United Kingdom, meaning that companies may transfer EU/UK personal data to the DIFC without putting in place a transfer mechanism (such as Standard Contractual Clauses). The New DP Law will apply to companies incorporated in the DIFC, regardless of where processing takes place, or companies that, whilst incorporated elsewhere, process personal data in the DFIC as part of stable arrangements (other than occasional processing). In the latter case, the New DP Law only applies to those processing activities taking place within the DIFC.

Whilst the New DP Law has incorporated many aspects of the EU's General Data Protection Regulation (GDPR), it does not take an identical approach with regard to sanctions which, under the GDPR, could potentially be up to €20 million or 4 percent of annual global turnover (whichever is greater). Under the New DP Law, the Commissioner of Data Protection may issue a general fine for contravention, and may, in addition, issue fines for specific contraventions, various limits of which are provided by a Schedule to the New DP Law (with the highest being $100,000). Data subjects also have the power to apply directly to the DIFC courts for compensation in the event of a contravention and, in addition, the Commissioner of Data Protection may order the payment of damages irrespective of whether a data subject has raised a claim.

The New DP Law mirrors the GDPR extensively, including by setting out the responsibilities and standards for both controllers-parties determining the purposes and means of processing-and processors-those processing personal data on behalf of a controller. It also mirrors the GDPR in the following ways:

Accountability Requirements: Controllers are required to put in place programs demonstrating compliance with the New DP Law, similar to the GDPR's accountability requirements. This program should include a data protection policy. Controllers and processors are also required to maintain a record of their processing activities and to implement the principle of "data protection by design and by default."

Data Protection Principles: The New DP Law sets out requirements for processing that are largely identical to the data protection principles under the GDPR, i.e., that personal data be processed lawfully, fairly and transparently, that it be processed for specified, explicit and legitimate purposes and processing be relevant and limited to what is necessary. Further, both laws require that personal data be accurate and kept up-to-date, kept in identifiable form only for the period necessary, and kept secure.

Lawful Bases for Processing: The New DP Law provides essentially the same legal bases for processing of personal data as the GDPR. Specifically, processing is lawful to the extent that it: (i) relies on the consent of the data subject; (ii) is necessary for the performance of a contract with the relevant data subject; (iii) is required by applicable law; (iv) is necessary to protect the vital interests of natural persons; (v) is necessary for the exercise of a DIFC authority's powers or functions; and (vi) is necessary for the purpose of a legitimate interest which is not overridden by the interests or rights of a data subject.

With regard to consent, the New DP Law reflects elements of the GDPR's standard, i.e., that the consent be freely given and demonstrated by a clear affirmative act showing an unambiguous indication of consent. The New DP Law does not specify that consent must be "informed" in the same way as the GDPR, but does require that it be provided for discrete processing purpose (similar to the requirement for specificity under the GDPR), and that data subjects be able to withdraw consent as easily as they provided it. Controllers are also required to implement appropriate and proportionate measures to assess the ongoing validity of the consent.

Data Subject Rights: Data subjects are provided certain rights in relation to their personal data, including rights: of access; of rectification; of erasure; to withdraw consent; to object to processing (an unqualified right where processing is for direct marketing purposes); to restrict processing; to data portability; and to object to, and require manual review of, any decision based solely on automated decision-making that produces legal or seriously impactful consequences. Controllers are also required to provide data subjects with information relating to their processing and an individual's rights with respect to their data.

Data Protection Officer (DPO): A DPO must be appointed to monitor and advise on compliance with the New DP Law where a controller or processor engages in "high risk processing activities" on a systematic or regular basis, the definition of which includes criteria that is similar, but not identical to, the criteria for appointment of a DPO under the GDPR. High risk processing activities are defined as those involving:

- adoption of new or different technologies or methods that materially increase the risk to the security or rights of data subjects or make it more difficult for data subjects to exercise their rights;
- significant amounts of personal data being processed, with such processing likely to result in a high risk to the data subject;
- systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, on which decisions are based that result in legal or similarly significant effects for the individual; or
- processing of material amounts of special category data (which has essentially the same definition as special category data under the GDPR).

Unlike the GDPR, DPOs are required to undertake annual assessments of a controller's processing activities for submission to the Commissioner of Data Protection.

Data Protection Impact Assessments: High risk processing activities also trigger the requirement for a controller to carry out a data protection impact assessment, and the controller is required to consult with the Commissioner of Data Protection where the assessment indicates that, even with mitigation, the risks to data subjects remain particularly high.

Data Transfers: The New DP Law prohibits transfers outside of the DIFC where the Commissioner of Data Protection has determined that the recipient jurisdiction, or a specified sector within the recipient jurisdiction (a deviation from the GDPR) provides an adequate level of data protection. Among the available safeguards that will permit such transfers are Standard Contractual Clauses or Binding Corporate Rules. The New DP Law also includes a derogation allowing for data transfers among government authorities, assuming that the controller takes reasonable steps to ensure the request is valid and proportionate, assesses and minimises the potential risks to data subjects and, where possible, obtains assurances from the requesting authority that the rights of data subjects will be respected and the data protection principles will be complied with.

Data Breach Notification: Controllers are required to notify the Commissioner of Data Protection of any personal data breach that compromises a data subject's confidentiality, security or privacy. Breaches must also be notified as to data subjects if the breach is likely to result in a high risk to the security or rights of data subjects.

Special Category Data: There is a general prohibition on processing of special category data unless a derogation applies. Again, these derogations mirror those set out under the GDPR, but the New DP Law provides some additional derogations, including processing that is proportional and necessary to protect data subjects from potential bias or inaccurate decision-making.

Controller-Processor Agreements: Controllers must put in place legally binding written agreements with processors to whom they disclose personal data, as under Article 28 of the GDPR, and processors are expected to execute the same agreements with sub-processors.

The New DP Law also incorporates certain aspects of the California Consumer Privacy Act of 2018 (CCPA) and its proposed regulations. Specifically, the NEW DP Law follows the CCPA in prohibiting businesses from discriminating against consumers for exercising their rights under the CCPA, including by offering a financial incentive or price or service difference (subject to certain exemptions). In addition, the CCPA provides consumers with the right to opt out of the "sale" of their personal information, a term that is broadly defined under the CCPA.

Hunton Andrews Kurth LLP will continue to monitor further developments in the New DP Law and share our insights and experience as our clients navigate the New DP Law-implementation process. Please feel free to contact the authors for further information and assistance.

Contacts

David Pang
dpang@HuntonAK.com

Olivia R. Lee
olee@HuntonAK.com

Jenna N. Rode
jrode@HuntonAK.com