Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

New DIFC Data Protection Law in Force – What You Need to Know

October 2, 2020

On October 1, 2020, the three-month grace period for businesses to comply with the Dubai International Financial Centre (DIFC) Data Protection Law (DIFC Law No. 5 of 2020) ("DPL 2020") came to an end. Regulating the processing of personal data in the DIFC, the DPL 2020 replaces the previous data protection law (DIFC Law No. 1 of 2007 (as amended) ("DPL 2007"))[1] and, significantly, brings the data protection regime in the DIFC closer in line to global data protection standards, notably the European Union General Data Protection Regulation (GDPR) and the U.S. California Consumer Privacy Act (CCPA). Although organizations already subject to the GDPR may be well placed to comply with the DPL 2020, it is recommended that organizations promptly begin reviewing their data processing activities to ensure they are in compliance with the DPL 2020. The financial and reputational consequences of failure to comply with the DPL 2020 are significant, including administrative fines of up to $100,000 and scope for larger, unlimited fines for serious violations of the DPL 2020.

Below, we outline some notable changes to the data protection regime and key features that entities should be aware of in light of the compliance deadline.[2]

1. Notable Changes and Key Features

Extraterritorial Reach

The DPL 2020 applies to (i) the Processing of Personal Data by a Controller or Processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not; and (ii) a Controller or Processor, regardless of its place of incorporation, that processes Personal Data in the DIFC (i.e. when the means or personnel used to conduct the Processing activity are physically located in the DIFC) as part of a "stable arrangement", other than on an occasional basis, and in the context of its processing activity in the DIFC. Previously, the DPL 2007 applied solely "in the jurisdiction of the DIFC" and thus the DPL 2020 extends the extraterritorial reach of the data protection regime. The DPL 2020's extraterritorial reach is not as expansive as the GDPR, because the GDPR applies to entities that are not established in the European Union when offering goods and services to or monitoring the activities of individuals in the Europe Union.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
Abu Dhabi
+971 2.406.8520

Jenny Arlington (nee Grozdanova)
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Mazen Baddar
Associate
mbaddar@akingump.com
Abu Dhabi
+971 2.406.8552

Sahar Abas
Associate
sahar.abas@akingump.com
Dubai
+44 20.7012.9859

New Data Subject Rights

The DPL 2007 provided Data Subjects with the right of access, rectification, erasure, to object to the processing of Personal Data under certain circumstances, and to block the processing of Personal Data that does not comply with the provisions of the law. The DPL 2020 adds to these existing rights by clarifying them and including provisions that appear to mirror certain provisions in the GDPR. For example, the DPL 2020 includes a right of access, which was provided for in the old regime, but specifies that a Data Subject must be provided with a copy of the Personal Data undergoing Processing without charge, within one month, and in electronic form.

Additionally, the DPL 2020 includes two provisions that are similar to the CCPA and the final draft of the California Attorney General's implementing regulations. First, the DPL 2020 specifies that a Controller must make available a minimum of two methods by which Data Subjects can contact the Controller to exercise their rights under the DPL 2020. These two methods must not be onerous and, if the Controller maintains a website, at least one method must be available without charge via the website and without requiring the Data Subject to create an account. Second, the DPL 2020 prohibits a Controller from discriminating against a Data Subject for exercising their rights under the DPL 2020, but does not prohibit a controller from offering financial or non-financial incentives for the processing of Personal Data provided that certain conditions are met.

Other notable new rights provided under the DPL 2020 include:

- The "absolute right" to withdraw consent at any time by notifying the Controller, where the Processing of Personal Data was carried out on the basis of consent (similar to Article 7 of the GDPR).
- The right to require the Controller to restrict Processing where certain conditions apply, such as where the accuracy of the Personal Data is contested by the Data Subject (similar to Article 18 of the GDPR).
- The right to receive the Personal Data provided to a Controller in a structured, commonly used and machine readable format where Processing is based on the Data Subject's consent or the performance of a contract and carried out by automated means. It also gives Data Subjects the right to request that a Controller transmit this data directly to another Controller, where technically feasible (similar to Article 20 of the GDPR).
- The right not to be subject to a decision based solely on automated Processing, which produces legal effects that significantly affect the Data Subject (similar to Article 22 of the GDPR).

Revised Consent Requirements

The DPL 2020 includes a new and more fulsome consent regime that mirrors the requirements found in the GDPR. Under the DPL 2020, consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent. A Controller must be able to demonstrate that consent was freely given and a Data Subject may withdraw their consent at any time. Importantly, a Data Subject's ability to withdraw his or her consent should not require undue effort and must be at least as easy as the process of giving consent. Once a Data Subject withdraws consent, the

relevant Controller must cease Processing the Data Subject's Personal Data and must securely and permanently delete it as soon as reasonably possible.

International Data Transfer

The DPL 2007 included limitations on transfers of Personal Data out of the DIFC, requiring that the country receiving the Personal Data maintains "an adequate level of protection" for Personal Data, as determined by the Commissioner of Data Protection ("Commissioner"), or that the transfer is made under certain conditions specified in the law. The DPL 2020 has retained the 2007 provision that such transfers are permitted to "adequate countries" but removed the possibility that a transfer could take place if the Commissioner has granted written authorization for the transfer. The DPL 2020 includes additional mechanisms for data transfers that are similar to those provided in the GDPR, such as the reliance on:

- A legally binding instrument between public authorities (similar to Article 46(2)(a) of the GDPR).
- Binding Corporate Rules, where the transfer is within the Controller's group and have been approved by the Commissioner (similar to Article 46(2)(b) of the GDPR).
- Standard data protection clauses as adopted by the Commissioner (similar to Article 46(2)(c) of the GDPR).
- An approved code of conduct together with binding and enforceable commitments of the Controller or Processor in the Third Country or International Organization to apply the appropriate safeguards, including with regard to Data Subjects' rights (similar to Article 46(2)(e) of the GDPR).
- An approved certification mechanism together with binding and enforceable commitments of the Controller or Processor in the Third Country or International Organization to apply the appropriate safeguards, including with regard to Data Subjects' rights (similar to Article 46(2)(f) of the GDPR).
- Where a transfer to a non-adequate country is not based on an adequate safeguard or a particular derogation, such a transfer may only take place if certain conditions are met, including where the transfer is necessary for purposes of "compelling legitimate interests pursued by the Controller."

Data Breach Provisions

The DPL 2007 included general security requirements, obligations for Controllers to select Processors that provide sufficient security guarantees in respect of security measures, and a general requirement to notify the Commissioner in the event of "an unauthorized intrusion, either physical, electronic or otherwise, to any Personal Data database." The DPL 2020 has added more explicit data breach provisions similar to the GDPR, requiring that Controllers notify the Commissioner if there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy. The provisions also include that Processors must notify Controllers, without undue delay, after becoming aware of a breach and requires Controllers to notify Data Subjects when a Personal Data Breach is likely to result in a "high risk to the confidentiality, security or privacy of Data Subjects."

Data Protection Impact Assessment Requirements and Data Protection Officers

The DPL 2020 introduces two requirements that are similar to those found under the GDPR where Controllers and Processors are engaged in High Risk Processing Activities. High Risk Processing Activities include the Processing of Personal Data with new technologies that create a materially increased risk to the security or rights of a Data Subject, sensitive Personal Data, Processing involving systematic and extensive evaluation of personal aspects relating to individuals or the processing of a material amount of Special Categories of Personal Data.

DIFC bodies must appoint a Data Protection Officer (DPO). Additionally, Controllers and Processors are required to appoint a DPO when they perform (or will commence performing) High Risk Processing Activities on a systematic or regular basis and must carry out a Data Protection Impact Assessment (DPIA) prior to engaging in any such activities.[3] The DPIA must include certain information and prior consultation with the Commissioner is required where the DPIA indicates that the risks to the rights of Data Subjects remain particularly high. Failure to appoint a DPO may result in a fine of $50,000. Where a DPO is required, they must undertake an assessment of the Controller's processing activities at least once per year, with the assessment also submitted to the Commissioner. The DPO must reside in the United Arab Emirates, unless employed within an organization's group and perform a similar function within the origination on an international basis.

Notably, the DPL 2020 specifies that if a Controller or Processor is not required to appoint a DPO, it must still "clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations."

Penalties

Under the DPL 2007, penalties ranged from $5,000 to $25,000 in respect of each contravention for nine specified violations. The DPL 2020 increases the range of fines and violations. As outlined in Schedule 2 of the DPL 2020, non-compliance is subject to penalties ranging from $25,000 to $100,000, depending on the violation and in respect of each infringement. The DPL 2020 also lists thirty-five different violations and fines.

Data Subjects and the Commissioner may bring an action for compensation (without any maximum cap) directly before the DIFC courts where material harm has been suffered as a result of a data breach. The Commissioner further retains the discretion to look beyond Schedule 2 in relation to serious breaches. In addition to financial repercussions, the Commissioner may issue public reprimands and this may have reputational consequences.

Other Notable Changes

Additional changes include:

- Consent to Process Personal Data from Data Subjects no longer needs to be specifically in written format (similar to Articles 4(11) and 7 of the GDPR). The new language leaves room for other forms of consent. Controllers are required to implement appropriate and proportionate measures to assess the ongoing validity of consent (except in limited cases); where such an assessment concludes that the Data Subject would no longer reasonably expect the processing to be continuing, the Data Subject must be contacted without delay and asked to re-affirm consent.

- Additional notice requirements where Personal Data is collected directly or indirectly from a Data Subject, including the lawful basis for processing and whether the Personal Data is to be transferred out of the DIFC (similar to Article 13 of the GDPR).
- Public authorities may not rely on legitimate interests to Process Personal Data (similar to Article 6(1) of the GDPR).
- Controllers and Processors must implement appropriate technical and organizational measures to ensure that Processing is performed in accordance with the DPL 2020 (similar to Article 24 of the GDPR).
- Processing by a Processor must be governed by a legally binding contract with the Controller that sets out specific provisions laid out in the DPL 2020 (similar to Article 28 of the GDPR). The ability of a Processor to appoint a Sub-processor is also limited absent certain requirements being met and Processors remain fully liable to the Controllers for the performance of the Sub-processor's obligations.
- Each Controller has to maintain a written record in electronic form of Processing activities that are under its responsibility, including the purpose of the Processing and a description of categories of Data Subjects and Personal Data (similar to Article 30 of the GDPR).
- The concept of Joint Controllers has been introduced where two or more Controllers jointly determine the purpose and means of processing. Joint Controllers must have a written agreement that determines their respective responsibilities for ensuring compliance with the obligations of the new data protection law (similar to Article 26 of the GDPR).

2. Key Takeaways

Due to the global pandemic, although the DPL 2020 entered into effect on July 1, 2020, the DIFC has confirmed that active enforcement will only commence on October 1, 2020. For those already operating or processing data in the DIFC, existing data protection compliance programs may need to be updated. Entities that already have measures in place to comply with the GDPR may be better suited but there are differences between the two regimes and this should be borne in mind.

As of October 1, 2020, if you operate in the DIFC you should consider the following:

- Map and audit Personal Data flows to determine whether you are within the scope of the DPL 2020 and how the changes to the law may affect your options.
- Determine if your company is a Data Controller and/or a Data Processor as you may have different responsibilities.
- Review existing agreements in place and determine whether you are compliant with the new requirements.
- Evaluate your company's privacy and data security requirements and determine whether measures are in place to comply with the law's Personal Data Breach notification requirements.
- Determine whether you engage in High Risk Processing Activities that require the appointment of a Data Protection Officer and/or a DPIA.
- Ensure you have processes in place to facilitate Data Subject requests.

- Determine and document your basis for Processing Personal Data and ensure that you are providing adequate notice to Data Subjects.
- Evaluate any cross-border data transfers and, where applicable, establish a valid mechanism through which such transfers can take place.

If you wish to enquire about further assistance with the DPL 2020 please do not hesitate to contact any members of the Akin Gump team.

[1] The DPL 2007 was amended in 2012 and 2018. A draft of the proposed law was introduced in June 2019. The changes to the DIFC data protection regime have followed an extensive 18-month consultation process led by the DIFC Office of the Commissioner.

[2] Capitalized terms used throughout this alert are as defined in the DPL 2020.

[3] Entities should also keep in mind that, under the DPL 2020, the Commissioner may establish a list of the kind of Processing operations for which no DPIA is required.

akingump.com