Pinsent Masons
بنسنت ماسونز

The new 2020 DIFC Data Protection Law

Summary Guide

Developing a robust framework to support the DIFC's bid for adequacy recognition by the European Commission, the United Kingdom and other jurisdictions around the world.

The new Data Protection Law, DIFC No. 5 of 2020 (the "DP Law"), comes into force on 1 July 2020 and replaces DIFC Law No.1 of 2007. Businesses caught by the legislation have a grace period of three months to bring their organisations into compliance with the new requirements.

As previously discussed here, the new DP Law has been aligned with data protection regimes elsewhere in the world such as the European GDPR and the California Consumer Privacy Act. Adoption of international data privacy concepts means we're hopeful that such reform will see other territories recognising the DIFC as providing sufficient regulatory protection to allow data transfers in and out of the DIFC with relative ease.

The DIFC Commissioner of Data Protection (the "Commissioner") has published a number of guides to assist firms with their implementation of the new requirements. These are not binding and do not have the force of law, but instead are indicative of the approach the Commissioner will take to enforcement. We are still awaiting publication of the supporting regulations.

This update picks up on some of the new developments in the data protection regime in the DIFC and highlights the need for businesses to become aware of their new compliance requirements as soon as possible in order to give ample time to prepare for the 1 October 2020 deadline.

Effect on non-DIFC businesses

The DP Law applies to:

I. all businesses incorporated in the DIFC who are processing personal data (regardless of where the personal data is being processed); and
II. any business which processes personal data in the DIFC as part of "stable arrangements", rather than just on occasion (regardless of the business' place of incorporation).

In this context, "in the DIFC" means when the personnel used to conduct the processing or the means of doing so are physically located in the DIFC.

Therefore, payroll providers, cloud software providers and other suppliers will need to be aware of their obligations under the DP Law. The enforcement of fines and damages imposed by the DIFC courts may be sought through the UAE court system.

Higher penalties for non-compliance

The Commissioner may issue fines for both administrative and more general contraventions which may be enforced through the courts if businesses fail to pay. In addition, a data subject may apply to the court for compensation if they suffer damage as a result of a breach of the DP Law.

For example, the maximum fines for failing to:

- notify the Commissioner of an unauthorised intrusion has increased from USD5,000 to USD50,000;

- implement and maintain technical and organisational measures to protect Personal Data has increased from USD10,000 to USD50,000; and
- maintain records of processing has increased from USD5,000 to USD25,000;
- In addition, a new number of new fines have been added, including fines of up to USD100,000 for failure to comply with the following:
- data subject rights of access, rectification and erasure of personal data;
- new requirements relating to data portability; and
- new right of a data subject to object to any decision based solely on automated processing, including profiling, which produces legal or other seriously impactful consequences.

The Commissioner has the power to inspect and audit businesses caught by the application of the DP Law in order to verify compliance.

Personal data

Personal data is any information referring to an identified or identifiable natural person.
Identified or Identifiable means, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

The references to "location data" and "online identifier" in the definition is new and similar to wording in the EU GDPR. Online identifiers may be IP addresses or cookie identifiers. Not all location data will be considered Personal Data within the DP Law; it will depend on the context. However, the broader definition may capture data not previously considered to be caught within the DIFC's data privacy's regime.

Rights of data subjects

The DP Law largely mirrors the rights granted to data subjects in the EU GDPR. Data subjects have various rights including the right to request copies of their personal data at any time, the right to rectify data and the right to withdraw consent and request erasure of their personal data.

One of the criticisms of the EU GDPR is that it fails to adequately allow for new emerging blockchain technologies where personal data is stored indefinitely and cannot be dealt with in the manner assumed by modern data protection laws. The DP Law seeks to remedy this by introducing an exemption from the right to rectify and erase personal data if the data controller discloses certain information to the data subject at the time of disclosure including that such personal data will be processed in a way that prevents the data subject from exercising such rights.

The DP Law also introduces a new right for data subjects not to suffer discrimination as a result of the exercise of their rights. This concept is derived from the recently enacted Californian Consumer Privacy Act and it will be interesting to note how this develops in practice. If a customer refuses to allow a business to retain its personal data, under the DP Law that business is required to provide the customer with the same quality of services/goods as other customers.

Data Protection Officers

A business conducting "High Risk Processing Activities" has additional compliance requirements including the requirement to appoint a Data Protection Officer. Data Protection Officers are responsible for monitoring compliance with the DP Law and other applicable privacy laws, act as a contact point for the Commissioner and oversee all data protection impact assessments. The contact details of the Data Protection Officer must be given to data subjects when collecting their personal data.

A Data Protection Officer may hold other roles or titles within the business provided such additional tasks and duties do not result in a conflict of interest or otherwise prevent the proper performance of the role. The role of Data Protection Officer may also be outsourced to an external party provided they have access to all relevant resources.

Generally, the DP Law requires the Data Protection Officer to be resident in the UAE, unless s/he is an individual employed by a Group of members and performs a similar function for the Group on an international basis elsewhere. In such cases, the Data Protection Officer must be easily accessible to each member in the Group.

The Data Protection Officer is required to complete an annual assessment and submit the same to the Commissioner. This is not intended to be an onerous obligation and will be integrated into existing DIFC compliance and reporting cycles.

The definition of "High Risk Processing Activities" pools together certain types of processing activity and includes:

(i) processing that includes the adoption of new or different technologies or methods which increase the risk to the security or rights of a data subject or renders it more difficult for a data subject to exercise its rights;

(ii) processing a large amount of personal data, including staff and contractor personal data, where such processing is likely to result in a high risk to the data subject;

(iii) systematic and extensive automated processing, including profiling, with significant effects; or

(iv) processing a material amount of sensitive data (referred to as "Special Categories of Personal Data").

The Commissioner has published comprehensive guidance and a list of activities that are considered to be High Risk Processing Activities here. Although this Guidance is comprehensive, it will often be a judgment call as to whether certain activities fall within the definition. Businesses should regularly assess whether their processing activities are caught within scope and stay on top of any updates issued by the Commissioner.

Failure to appoint a Data Protection Officer when required or requested to do so may result in a fine of up to USD50,000.

Breach notifications

Breach notifications to the Commissioner

Under the DP Law, a "Personal Data Breach" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If such a Personal Data Breach compromises a data subject's right to security or confidentiality, then expeditious notifications are required.

Personal data breaches may include the infiltration of an IT system by a virus or third parties, an employee leaking information to third parties, incorrect use of email, stolen or lost laptops or devices. This is a much wider definition than the previous DIFC data privacy regime which merely required notifications to the Commissioner in the event of an "unauthorised intrusion" to a personal data "database".

The new DP Law does not include any 'de minimus' limits for which a report must be made, so a strict technical interpretation of the requirements suggests that any breach (however small) would trigger a notification requirement to the Commissioner.

Any business who processes information on behalf of a "Controller" (being any person who determines the purposes and means of processing personal data) must notify the Controller of the Personal Data Breach "without undue delay". A Controller must notify the Commissioner of the Personal Data Breach "as soon as

reasonably practicable". Failure to so notify may result in a fine of up to USD50,000 on either or both of the Controller and Processor.

As well as including details of the number of data subjects affected and the likely consequences of the data breach, the Controller's notification to the Commissioner must also include details of measures taken or proposed to be taken to mitigate the adverse affects of the Personal Data Breach. However, in order to avoid the delay of the original notification, such information may be provided at a later time, when available.

Breach notifications to data subject

A new requirement to notify data subjects has also been introduced in line with the requirements in the GDPR. Notification is required if it is "likely to result in high risk to the security or rights" of the data subject. A Controller must make such notification as soon as practicable. However, if there is an "immediate risk of danger", such notification must be made promptly.

The DP Law also contains a derogation such that where a notification to an affected data subject may involve a disproportionate effort, a public communication or similar measure will be sufficient to satisfy the new provisions. Failure to notify in accordance with these requirements may result in a fine of up to USD50,000. A data subject may also apply to the court for compensation or damages where they have suffered loss as a result of the failure to notify.

Written agreements required for processors

Where services involving the processing of personal data are provided by other parties, contracts must contain much more robust contractual provisions. If the service provider appoints another company to carry out such services, then they must obtain the consent of the Controller and the sub-contract must also contain similar robust contractual provisions.

Such contractual provisions must include commitments to:

- process the personal data following documented instructions from the Controller;
- permit and assist with audits and inspections and make certain information available upon request by the Commissioner, the counterparty or an auditor;
- ensure that all persons authorised to process personal data are under legally binding written agreements or duties of confidentiality;
- keep a program that demonstrates compliance with the Law; and
- provide appropriate technical and organisational measures to meet the Controller's obligation to respond to requests from data subjects.

The Commissioner may publish standard contractual provisions for businesses to use in their contracts.

Failure to ensure that such contracts are in place with all relevant processors of personal data may result in a fine of up to USD25,000.

Immediate actions:

Complying with the new requirements in the DP Law is not something that can be left solely to the responsibility of your Legal and Compliance teams. Instead, compliance with your data privacy obligations requires everybody in your organisation to understand their role and responsibility to keep your data safe and secure.

Our cross sector regulatory team is well placed to support you with your organisation's compliance with the new DP Law. We have identified below a number of areas we can assist you with. If you have any questions, or

would like an informal discussion on some of the themes raised above, please do not hesitate to reach out and contact a member of the team.

- Review your current and future planned processing activities to identify what personal data you collect and ensure that it is being processed in accordance with a legitimate reason, including that it is relevant, accurate and being processed for the specific purpose for which it was collected and that all justifications for processing such data (including data subject consents, where relevant) remain valid;
- Populate registers of processing activities that record personal data use;
- Update privacy notices and customer facing terms and conditions to address the changes in the new DP Law (for example, alerting customers to their new data subject rights);
- review and remediate your existing controller / processor contractual arrangements - putting contracts into place with processors that contain the mandatory provisions as required by the DP Law;
- Evaluate whether you are conducting "High Risk Processing Activities" and consider appointing a Data Protection Officer;
- Review the terms of your employment contracts;
- Implement new data breach procedures to ensure that notifications are made to the Commissioner and data subject, as required, in a timely manner in accordance with the DP Law;
- Establish processes for dealing with data subject requests within the time required; and
- Raise internal awareness of new requirements.
- If you have any questions on the contents of this Guide, please do reach out.

Your Key Contacts at Pinsent Masons

Tom Bicknell
Partner
M: +971 56 403 8136
tom.bicknell@pinsentmasons.com

Marie Chowdhry
Senior Associate
M: +971 50 219 3625
marie.chowdhry@pinsentmasons.com

Tom is the Head of Pinsent Masons' Financial Services Practice in the Middle East. He has worked in the region for seven years and has over twelve years' experience in financial services. Tom has worked with regulators across the UAE to undertake benchmarking and regulatory analysis studies across the onshore and freezone market.

Tom works with a number of international and regional businesses focussed on the transformative effects of financial technology and has a particular focus on the use of digital assets throughout the global financial sector.

Tom is recognised as a **Leading Individual** in the recent UAE 2020 Legal 500 rankings, which describe him as a '**superstar**', '**client focused and highly responsive**'.

Marie is a versatile regulatory and payments lawyer with experience advising banking and insurance clients, payment service providers, and FinTech start-ups on all aspects of their business and operations throughout the Middle East. Marie provides advice on all licensing matters arising across the GCC, with particular focus on KSA, UAE and Bahrain (including both onshore and freezone regimes).

Marie's extensive experience acting on regulatory-led transformation programmes gives her an excellent overview of what is required to bring complex regulatory-led programmes to successful completion.

Marie has been identified as a **Rising Star** in the recent UAE 2020 Legal 500 rankings, which describe her as '***exceptional in her field of expertise***'.