DIFC DATA PROTECTION LAW – ACTIONS REQUIRED BY BUSINESSES

EXECUTIVE SUMMARY

The Dubai International Financial Centre ("**DIFC**") Data Protection Law 2020 (DIFC Law No. 5 of 2020) (the "**Law**") and the DIFC Data Protection Regulations (the "**Regulations**") came into force on 1st July 2020 in response to the rapid global technological changes.

The DIFC announced that businesses had until 1st October 2020 to bring their operations into compliance with the new requirements, as after this time, the Data Commissioner may take enforcement action for any failures to comply with the Law and Regulations.

The purpose of the Law is to provide standards and controls for the Processing and free movement of Personal Data by a Controller or Processor and to protect the fundamental rights of Data Subjects.

The Law brings the DIFC in line with other data protection regimes elsewhere in the world, including the EU General Data Protection Regulation ((EU) 2016/679) ("**GDPR**") which replaced the regime established by the Data Protection Act 1998.

This article highlights the key provisions of the Law so that businesses are aware of them and the steps that need to be taken to ensure compliance.

WHAT IS THE SCOPE?

In addition to any business registered in the DIFC, the Law applies to:

(1) any business which processes Personal Data within the DIFC "*as part of stable arrangements*"; and

(2) any business which processes data on behalf of a business incorporated in the DIFC (regardless of whether the Processing takes place inside the DIFC or outside).

Under the Law, processing "*in the DIFC*" occurs when the means or personnel used to conduct the processing activity are physically located in the DIFC, and processing "*outside the DIFC*" is interpreted accordingly.

WHAT IS PERSONAL DATA?

Personal Data is defined as "*any information referring to an identified or Identifiable Natural Person*".

"*Identified Natural Person*" means a natural living person who can be identified, 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 or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

The Law provides that Personal Data must be processed in accordance with the application of Data Subject rights and processed in a transparent manner, and explains that Special Categories of Personal Data shall not be processed unless certain conditions apply, as listed under the Law.

WHAT ARE THE REQUIREMENTS?

A Controller or Processor is any person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Controllers and Processers must now both be able to demonstrate their compliance with the data protection principles in the Law, as follows:

(1) Appoint a Data Protection Officer (see below);
(2) Ensure consent is freely given;
(3) Ensure a lawful basis for processing;
(4) Establish Data Protection Impact Assessments ("DPIA") for High Risk Processing Activities (see below) and ensure consultation with the Commissioner where a DPIA is required;
(5) Lawful, fair and transparent processing, in accordance with Data Subjects' rights;
(6) Maintain records by Controllers and Processors;
(7) Register with the Commissioner, establish a compliance program for the Law and appropriate technical and organizational measures, and implementation of privacy design and by default;

Breach notifications are required:

(1) to the Data Subject - for Personal Data Breaches which are likely to result in a high risk to the security or rights of a Data Subject, the Controller must communicate the Personal Data Breach to an affected Data Subject as soon as practicable in the circumstances; and

(2) to the Commissioner - as soon as practicable in the circumstances if there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy (section 41 of the Law)

Processors and Sub-Processors requirements are as follows:

(1) Authorisation from Controllers for Sub-Processors – to inform Controllers of any intended changes relating to the addition or the replacement of a Sub-Processor; and

(2) Legally Binding Agreements – are required between Data Processor and Sub-Processors.

APPOINT A DATA PROTECTION OFFICER

Businesses must appoint a Data Protection Officer for:

(1) DIFC bodies (other than the courts acting in their judicial capacity);

(2) Controllers or processers performing “high-risk processing activities” (as indicated below) on a systemic or regular basis; and

(3) As required by the Commissioner.

WHAT ARE HIGH RISK PROCESSING ACTIVITIES?

High Risk Processing Activities includes processing of Personal Data where one or more of the following applies:

(1) Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights;

(2) A considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data;

(3) The Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or

(4) A material amount of Special Categories of Personal Data is to be Processed.

WHAT ARE THE RIGHTS OF DATA SUBJECTS?

One of the main changes introduced by the Law is the enhancement of data subject rights with reference to personal data by clarifying the scope of existing rights and giving additional rights.

The Law includes the rights detailed in the DIFC Data Protection Law 2007 below:

(1) Right to rectification of personal data;
(2) Right to access personal data;
(3) Right to erasure or blocking of personal data; and
(4) Right to object to the processing of personal data under certain circumstances.

The Law now includes additional rights, as follows:

(1) Right to access within 1 to 2 months depending on the complexity of the request;
(2) Right to withdraw consent at any time;
(3) Right to object to automated decision making, including profiling;
(4) Right to data portability – the right to receive a copy of your own personal data; and
(5) Right to non-discrimination when the data subject exercises any of their rights.

CONSENT AND LEGITIMATE INTERESTS

Under the Law, Consent must be freely given and unambiguous. Consent can be withdrawn by the Data Subject at any time.

DATA EXPORT AND SHARING

An adequate level of protection is required for the transfer and sharing of data outside the DIFC.

The Law permits data transfer to pre-approved jurisdictions listed on the DIFC website; however, in the context of transfers to other jurisdictions, the Law provides companies with more options than the previous law and offers detailed guidance as to what constitutes adequate safeguards.

WHAT ARE THE FINES, LIABILITY AND SANCTIONS?

The Commissioner has the power to issue fines for contraventions of the Law by a Controller or Processor, in an amount they consider to be appropriate and proportionate.

The Law sets out the maximum fine of USD 100,000 for administrative breaches, with additional scope for larger fines for more serious violations.

The list of administrative fines under Schedule 2 of the Law are, as follows:

Contravention	Maximum Fine (USD)
Failure to register with the Commissioner	USD 25,000
Failure to appoint a Data Protection Officer	USD 50,000
Failure to notify the Commissioner of an unauthorized data intrusion	USD 50,000
Failure to implement and maintain technical and organisational measures to protect personal data	USD 50,000
Failure to maintain records of any Personal Data Processing operations	USD 25,000
Failure to carry out a data protection impact assessment prior to High Risk Processing Activities	USD 20,000

The Commissioner can issue such fines from 1st October 2020 onwards. Further, the Law permits compensation claims to be made by or on behalf of data subjects.

NEXT STEPS?

Our aim is to assist businesses by providing guidance on data protection, and the impact of the new regulations on their business strategies and models. We also advise employers that have not reviewed their employee policies, contracts, and data processing regimes to ensure these are up to date and in compliance with the Law.

If you require any assistance, please do not hesitate to contact us.

Robert Whitehead | Senior Associate
Hamdan Al Shamsi Lawyers & Legal Consultants

For any enquiry please click here