Delivering expert knowledge to global counsel

International Law Office®

Information Technology - United Arab Emirates

Implementation of Data Protection Law in DIFC

Author

Pier Terblanche

July 17 2007

Introduction
General Obligations
International Transfer Provisions
Recordkeeping and Notification Obligations
Non-compliance

Introduction

In January 2007 the Dubai International Financial Centre (DIFC), an international financial free zone located in Dubai, promulgated the Data Protection Law 2007, which abrogated the DIFC Data Protection Law 2004. In March 2007 the Data Protection Regulations 2007 followed, which repeal the Data Protection Module issued by the Dubai Financial Services Authority in 2004. This is the first substantial data protection legislation within the Gulf Cooperation Council region.

The new Data Protection Law provides a legal and procedural framework for ensuring that all personal data (ie, any information relating to an identifiable natural person) and sensitive data (eg, information about a person's political affiliation or racial identity) in the DIFC is treated fairly, lawfully and securely when it is stored, processed, used, disseminated or disclosed. The law applies only within the jurisdiction of the DIFC and is based largely on EU law and international standards (in particular the EU data protection directives and the guidelines of the Organization for Economic Cooperation and Development). It represents an effort on the part of the DIFC to comply with its stated intention to uphold international best practice. Administration of the law is the responsibility of the commissioner of data protection, who is appointed by the president of the DIFC (Article 21(1) of the law).

On May 29 2007 the commissioner issued an enforcement and compliance notice requiring all DIFC entities, whether regulated by the Dubai Financial Services Authority or not, to register by June 30 2007 and to "comply with all applicable provisions of the law" or face "fines and penalties".

General Obligations

A 'data controller' (defined as any entity in the DIFC that collects, records, organizes, uses, discloses or deals with personal data) must ensure that the data it processes is:

- processed fairly, lawfully and securely;
- processed for specified, explicit and legitimate purposes in accordance with the applicable data subject's rights;
- adequate, relevant and not excessive in relation to the purposes for which it is collected;
- accurate and up to date; and
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data was collected or for which it is further processed (Article 8(1)).

All reasonable steps must be taken by data controllers to ensure that personal data which is inaccurate or incomplete, with regard to the purposes for which it was collected or for which it is further processed, is erased or rectified (Article 8(2)).

Personal data may be processed only if:

- the data subject has given his or her written consent;

- it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- it is necessary for compliance with any legal obligation to which the data controller is subject;
- it is necessary in order to protect the vital interests of the data subject;
- it is necessary for the performance of a task carried out in the interests of the DIFC, the Dubai Financial Services Authority, the DIFC Court or in the exercise of the commissioner's functions or powers vested in the data controller or in a third party to which the personal data is disclosed; or
- it is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party to which the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to his or her particular situation (Article 9(1)).

'Sensitive personal data' is defined as personal data which reveals or concerns the data subject's:

- racial or ethnic origin;
- communal origin;
- political affiliations or opinions;
- religious or philosophical beliefs;
- criminal record;
- trade-union membership; or
- health or sex life (Article 3 of the Schedule to the law).

It may not be processed unless:

- the data subject has given his or her written consent;
- processing is necessary to carry out the obligations and specific rights of the data controller;
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body on condition that the processing relates solely to the members of that body or to persons who have regular contact with it in connection with its purposes, and that the personal data is not disclosed to a third party without the consent of the data subject;
- processing relates to personal data which is manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject;
- processing is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that it is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the data subject relating to his or her particular situation;
- processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter-terrorist financing obligations, or the prevention or detection of any crime that applies to a data controller;
- processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care treatment or the management of health-care services, and is undertaken by a health professional subject under national laws or regulations established by national competent bodies subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;

- processing is authorized in writing by the commissioner; or

- processing is required to protect members of the public against: (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons involved in the provision of banking, insurance, investment, management consultancy, IT, or accounting services or other commercial activities (either in person or indirectly by means of outsourcing); or (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons involved in the provision of banking, insurance, investment, financial or other services (Article 10(1)).

Article 10(1) will not apply if a permit has been obtained from the commissioner to process sensitive personal data and the data controller applies adequate safeguards with respect to the processing of the sensitive personal data (Article 10(2)). Article 16(1) may assist in determining what would constitute 'adequate safeguards', as it requires a data controller to:

"*implement appropriate technical and organizational measures to protect personal data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.*"

Such measures "shall ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected" (Article 16(2)).

International Transfer Provisions

Owners and managers of DIFC entities should take particular care to ensure compliance with the provisions of the law regarding the transfer of personal data outside of the DIFC to other countries. Pursuant to Article 11, and unless a condition as set out in Article 12(1) (see below) is satisfied, personal data may be transferred only to countries that offer an "adequate level of protection for that personal data" (Article 11 (1a)), which is the same standard as is imposed by the EU data protection directives. Although Article 11(2) states that a list of such countries is to be published in the regulations, the current regulations do not yet contain such a list. The expectation is that the European Union's list of 'certified' countries will be adopted by the DIFC.

Pursuant to Article 12(1), a transfer of personal data to a country whose laws do not ensure an adequate level of protection within the meaning of Article 11 may take place if:

- the commissioner has granted a permit or written authorization for such a transfer and the data controller applies adequate safeguards with respect to the protection of the data;

- the data subject has given his or her written consent to the proposed transfer;

- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken in response to the data subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the data controller and a third party;

- the transfer is necessary or legally required in the interests of the DIFC, or for the establishment, exercise or defence of legal claims;

- the transfer is necessary in order to protect the vital interests of the data subject;

- the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled;

- the transfer is necessary for compliance with any legal obligation to which the data controller is subject or is made at the request of a regulator, the police or another government agency;

- the transfer is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that it is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the data subject relating to the data subject's particular situation; or

- the transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter-terrorist financing obligations, or the prevention or detection of any crime that applies to a data controller.

Recordkeeping and Notification Obligations

A data controller must record the following information in relation to its personal data processing operations:

- a description of the processing;
- an explanation of the purpose of the processing;
- the identity of the data subject whose personal data is being processed;
- a description of the class of personal data; and
- the jurisdiction(s) to which the personal data may be transferred and an indication of whether such jurisdiction(s) has been assessed as having adequate protection for the purposes of Articles 11 and 12 of the law (Article 6(1)(i) of the regulations).

A data controller must notify the commissioner of any personal data processing operations involving (i) sensitive personal data, and (ii) the transfer of personal data to a country which does not have laws that ensure an adequate level of protection of such data (Article 6(2)(i) of the regulations). Such notification must contain:

- a description of the processing being carried out;
- an explanation of the purposes of the processing;
- the identity of the data subject;
- a description of the class of data being processed; and
- details of the country to which the data will be transferred (Article 6(2)(2) of the regulations).

Notification must be provided to the commissioner:

- immediately upon commencing the data processing;
- on every anniversary of the initial notification (if the processing continues into the subsequent year); and
- immediately upon any processing being performed in a manner which differs from that described in the initial notification (Article 6(3)(3) of the regulations).

Data controllers also have a duty to provide a data subject whose personal data they collect (whether directly from the data subject or otherwise) with at least the information set out in Articles 13(1) and 14(1) of the law, which includes the identity of the data controller and the purpose of the processing.

Non-compliance

Pursuant to Article 32(1) of the law, if the commissioner, after duly conducting all reasonable and necessary inspections and investigations, is satisfied that a data controller has contravened or is contravening the law or the regulations, he or she may issue a direction requiring the data controller to refrain from: (i) acting for such period as may be specified in the direction; and/or (ii) processing any personal data specified in the direction or for a purpose or in a manner specified in the direction.

The data controller may seek a review by the commissioner or the DIFC Court of the commissioner's decision to issue the direction (Articles 32(3) and 32(5)).

If the data controller fails to comply with the direction, it may be subject to fines and liable for payment of compensation. Although Article 27(2) provides for regulations to be issued in respect of fines, no such regulations have yet been published.

In addition, a data subject who believes on reasonable grounds that he or she has been adversely affected by a contravention of the law in respect of the processing of his or her personal data may lodge a complaint with the commissioner, who may mediate between the data subject and the relevant data controller (Articles 33(1) and (2)), and may issue a direction requiring the data controller to do what the commissioner considers appropriate (Article 33(3)).

Any data controller that is found to contravene the law or a direction of the commissioner may appeal to the DIFC Court, which will have the right to make such orders as it deems just and appropriate in the circumstances, including remedies for damages, penalties or compensation (Articles 34(1) and (2)). Article 35 specifically provides that:

"*a data subject who suffers damage by reason of any contravention by a data controller*

of any requirement of this law or the regulations is entitled to compensation from the data controller for that damage."

While it remains to be seen how strictly the law will be enforced, the mere fact that the 2004 Data Protection Law has been repealed and replaced with the 2007 law appears to indicate the DIFC's renewed intention to enforce data protection measures within its jurisdiction. DIFC entities would be well advised to comply with the enforcement and compliance notice, or else face undisclosed fines and penalties.

For further information on this topic please contact Pier Terblanche at Key & Dixon by telephone (+97 14 332 3324) or by fax (+97 14 332 3325) or by email (pier.terblanche@keydixon.com).