

DATA PROTECTION LAWS OF THE WORLD

UAE - Dubai (DIFC)



Downloaded: 11 July 2017

UAE - DUBAI (DIFC)



Last modified 24 January 2017

LAW

Note: Please also see [UAE – General](#).

The DIFC implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007 which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law ('DPL').

In addition, under the powers granted to the Commissioner of Data Protection ('CDP') under Article 27 of the DPL, the CDP has issued the Data Protection Regulations ('DPR').

DEFINITIONS

Definition of Personal Data

Any data referring to an Identifiable Natural Person

Definition of Identifiable Natural Person

Is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.

Definition of Process, Processed, Processes and Processing

Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection ('CDP') is essentially the regulating body in the DIFC.

The Data Protection Commissioner
Dubai International Financial Centre Authority

Level 14, The Gate
P.O. Box 74777
Dubai
United Arab Emirates

administrator@dp.difc.ae

Tel: +971 4 362 2623
Fax: +971 4 362 2656

REGISTRATION

Unless certain exceptions apply, Data Controllers must obtain a permit from the CDP prior to commencing a Processing Operation involving either Sensitive Personal Data or transferring Personal Data outside of the DIFC.

Data Controllers must also notify the CDP of any Processing operations involving either Sensitive Personal Data or the transfer of Personal Data outside of the DIFC.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR, for organisations to appoint a data protection officer, though note the general obligation of a Data Controller to implement appropriate technical and organisational measures to protect Personal Data, as further detailed below (see separate **Security** section).

COLLECTION & PROCESSING

Data Controllers may collect and process Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Personal Data (DPL, Article 9(a))
- processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (DPL, Article 9(b))
- processing is necessary for compliance with any legal obligation to which the Data Controller is subject (DPL, Article 9(c))
- processing is necessary for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFC Authority, the Dubai Financial Services Authority, the Court and the Registrar's functions or powers vested in the Data Controller or in a third party to whom the Personal Data are disclosed (DPL, Article 9(d)), or
- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation (DPL, Article 9(1)(e)).

Data Controllers may collect and process Sensitive Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Sensitive Personal Data (DPL, Article 10(1)(a))
- processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller (DPL, Article 10(1)(b))
- 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 consent (DPL, Article 10(1)(c))
- 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 the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects (DPL, Article 10(1)(d))

- the Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims (DPL, Article 10(1)(e))
- processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject (DPL, Article 10(1)(f))
- processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such 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 the Data Subject's particular situation (DPL, Article 10(1)(g))
- 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 apply to a Data Controller (DPL, Article 10(1)(h))
- processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Personal Data is Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (DPL, Article 10(1)(i))
- processing is required for protecting members of the public against dishonesty, malpractice or other seriously improper, or any resultant financial loss (DPL, Article 10(1)(j)), or
- authorised in writing by the CDP (DPL, Article 10(1)(k)).

TRANSFER

Data Controllers may transfer Personal Data out of the DIFC if the Personal Data is being transferred to a Recipient in a jurisdiction that has laws that ensure an adequate level of protection for that Personal Data (DPL, Article 11(1)(a)). An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the CDP (DPL, Article 11(2)).

In the absence of an adequate level of protection, Data Controllers may transfer Personal Data out of the DIFC if the:

- CDP has granted a permit or written authorisation for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of this Personal Data (DPL Article 12(1)(a)). Article 5.1 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of Personal Data for which the permit is being sought and including a description of the nature of the Personal Data involved)
- data Subject has given his/her written consent to the proposed transfer (DPL, Article 12(1)(b))
- transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request (DPL, Article 12(1)(c))
- transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a third party (DPL, Article 12.1(d))
- transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims (DPL, Article 12.1(e))

- transfer is necessary in order to protect the vital interests of the Data Subject (DPL, Article 12.1(f))
- transfer is made from a register which according to laws or regulations is intended to provide information to the public and which 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 in law for consultation are fulfilled in the particular case (DPL, Article 12(1)(g))
- transfer is necessary for compliance with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, police or other government agency (DPL, Article 12(1)(h))
- transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such 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 (DPL, Article 12(1)(i)), or
- 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 (DPL, Article 12(1)(j)).

Authorities who may receive Personal Data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

Safe Harbor Ruling - October 2015

On 26 October 2015 the CDP issued a [guidance](#) to DIFC registered entities regarding the adequacy status of US Safe Harbor recipients.

The guidance was issued as a result of a decision by the European Court of Justice (ECJ) on 6 October 2015 which invalidated the European Commission's Decision 200/520/EC. That EC Decision had provided "adequate protection status" for personal data transfers from European Member States to US Safe Harbor recipients.

As noted above, DPL, Article 11 allows a transfer of personal data out of the DIFC if:

1. an adequate level of protection for that personal data is ensured by the laws and regulations that are applicable to the recipient; or
2. in accordance with DPL, Article 12.

Like the European Commission, the DIFC Data Commissioner had previously listed the US Safe Harbor scheme as a jurisdiction with an "adequate level of protection" on its website. The US Safe Harbor scheme has however now been removed from that list.

The DIFC Data Commissioner's guidance observes that, as the DIFC Data Protection Laws are largely modelled on relevant EU Directives, the ECJ decision has caused the DIFC Data Commissioner to reconsider the adequacy status previously provided to US Safe Harbor rules. It has noted however that there are currently ongoing negotiations between EU and US authorities regarding the framework.

In light of the above, the DIFC Data Commissioner warns that DIFC organisations should continue to protect individuals' personal data when transferred to the US and consider potential risks by implementing appropriate legal and technical solutions in a timely manner. DIFC entities transferring personal data to the US should rely upon the conditions referred to in DPL, Article 12 until further clarity is provided.

It is expected that the CDP will release further guidance on how DIFC entities should navigate the Data Protection Law to enable them to legally transfer personal data to the US in the near future.

SECURITY

Data Controllers must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where Sensitive Personal Data is being Processed or where the Personal Data is being transferred out of the DIFC (DPL, Article 16(1)). When applying for a permit to Process Sensitive Personal Data, or Transfer Personal Data out of the DIFC, Data Controllers must include detail regarding the safeguards employed to ensure the security of such Sensitive Personal Data/Personal Data (respectively, Articles 2.1.1(i) and 5.1.1(i) of the DPR).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected (DPL, Article 16(2)).

BREACH NOTIFICATION

In the event of a breach (being an unauthorised intrusion, either physical, electronic or otherwise, to any Personal Data database, as defined by the DPL) Data Controllers (or Data Processors carrying out a Data Controller's function at the time of the breach), must inform the CDP of the incident as soon as reasonably practicable (DPL, Article 16(4)).

ENFORCEMENT

In the DIFC, the CDP oversees the enforcement of the DPL (DPL, Article 26).

The CDP needs to conduct all reasonable and necessary inspections and investigations before notifying a Data Controller that it has breached or is breaching the DPL or any regulations (DPL, Article 33). If the CDP is satisfied with the evidence of the breach, the CDP may issue a direction to the Data Controller requiring it to do either or both of the following:

- do or refrain from doing any act or thing within such time as may be specified in the direction (DPL, Article 33(1)(a)), or
- refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction (DPL, Article 33(1)(b)).

A Data Controller may ask the CDP to review the direction within fourteen days of receiving a direction and the CDP may receive further submissions and amend or discontinue the direction (DPL, Article 33(6)).

A Data Controller that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation (DPL, Article 33(4)).

In addition, if the CDP considers that a Data Controller or any officer of it has failed to comply with a direction, he may apply to the Court for one or more of the following orders:

- an order directing the Data Controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the CDP relevant to the issue of the direction (DPL, Article 33(5)(a))
- an order directing the Data Controller or officer to pay any costs incurred by the CDP or other person relating to the issue of the direction by the CDP or the contravention of such Law, Regulations or legislation relevant to the issue of the direction (DPL, Article 33(5)(b)), or
- any other order that the Court considers appropriate (DPL, Article 33(5)(c)).

Any Data Controller who is found to contravene the DPL or a direction of the CDP may appeal to the DIFC Court within 30 days (DPL, Article 37(1)). The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation (DPL, Article 37(2)).

ELECTRONIC MARKETING

As soon as possible upon beginning to collect Personal Data, the DPL requires Data Controllers to provide Data Subjects who they have collected Personal Data from, with, amongst other things, any further information to the extent necessary (having

regard to the specific circumstances in which the Personal Data is collected). This includes information on whether the Personal Data will be used for direct marketing purposes (DPL, Article 13).

If the Personal Data has *not* been obtained from the Data Subject, the Data Controller or their representative must at the time of undertaking the Processing – or if it is envisaged that the Personal Data will be disclosed to a Third Party, no later than when the Personal Data is first Processed or disclosed – provide the Data Subject with, amongst other things, information regarding whether the Personal Data will be used for direct marketing purposes (DPL, Article 14).

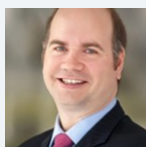
Before Personal Data is disclosed for the first time to third parties or used on a Data Subject's behalf for the purposes of direct marketing, Data Subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (DPL, Article 18).

Additionally, the DPL requires a Data Controller to record various types of information regarding its Personal Data Processing operations (Article 19(4)). This must include an explanation of the purpose for the Personal Data Processing (DPL, Article 6.1.1(b)). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the Data Controller itself or for others (Article 6.2.1).

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the DIFC, the privacy principles laid out therein may apply (see **UAE - General** section).

KEY CONTACTS



Paul Allen

Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com



Eamon Holley

Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com



Jamie Ryder

Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com



Robert Flaws

Senior Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.