DIFC DATA PROTECTION POLICY GUIDANCE
Commissioner of Data Protection

GUIDE TO

DATA PROTECTION LAW, DIFC LAW NO. 5 OF 2020

AND

DATA PROTECTION REGULATIONS

Disclaimer

The goal of the Commissioner of Data Protection ("Commissioner") in producing this document is to provide easy to understand information about the Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law") and the updated Data Protection Regulations (the "Regulations") (collectively the "Legislation").

The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm. The information, which may be amended from time to time, does not constitute legal or any other type of advice and it is provided for information purposes only.

If you require further information, please contact:

Office of the Commissioner of Data Protection
Dubai International Financial Service Authority
Level 14, The Gate
PO Box 74777, Dubai, UAE

Tel : +971 4 362 2223

Website: https://www.difc.ae/business/operating/data-protection/

Email: commissioner@dp.difc.ae

Contents

PART 1 OF THE DP LAW: INTRODUCTION AND GENERAL CONSIDERATIONS 1
What is Personal Data?.....1
What is an Identifiable Natural Person? 1
What is Special Category Data?.....1
What is Processing? 2
Who is a Data Subject?.....2
Who is a Controller? 2
Who is a Processor?.....3
Who is a Third Party? 3
What determines whether "information relates to an identified natural Person or Identifiable Natural Person"? 3
How does the Commissioner determine if a natural Person is capable of being "identified"? 4
Can Personal Data be anonymised?.....4
What about expressions of opinion?.....4

PART 2 OF THE DP LAW: GENERAL REQUIREMENTS - CORE PROVISIONS 4
Operation of the Legislation.....5
Security of Processing.....11
Policies, Compliance Program, Design and Default and Preferences.....13
Notifications to the Commissioner 13
Records of Processing Activities.....14
Designation of the DPO 14
DPIAs 15
Prior Consultation.....16
Cessation of Processing.....16

PART 3 OF THE DP LAW: OBLIGATIONS OF CONTROLLERS AND PROCESSORS 16
PART 4 OF THE DP LAW: DATA EXPORT AND SHARING 17
What is an adequate level of protection? 17
Standard Data Protection Clauses.....18
Data Sharing.....19

PART 5 OF THE DP LAW: INFORMATION PROVISION.....19

PART 6 OF THE DP LAW: RIGHTS OF DATA SUBJECTS 20
Protection of rights 20
Key rights of Data Subjects.....20
Right of subject access 21
Right to prevent Processing for the purpose of direct marketing 22

PART 7 OF THE DP LAW: PERSONAL DATA BREACHES 22

PARTS 8, 9 AND 10 OF THE DP LAW: COMMISSIONER'S POWERS AND APPLICABLE REMEDIES.....23
The Commissioner's powers.....23
Application to the Court and Compensation.....23
Mediation 23
Directions 23
Imposition of Fines 24
Powers to make rules about exemptions 24

PART 1 OF THE DP LAW: INTRODUCTION AND GENERAL CONSIDERATIONS

The Commissioner is responsible for administering the Legislation in Dubai International Financial Centre (DIFC). The Legislation provides a framework in which Personal Data may be collected, used, stored and transferred to other jurisdictions outside the DIFC or individuals with similar levels of protection. In order to fully understand the operation of the Legislation one must understand the concepts of Personal Data, Special Category Data, Processing, Data Subject, Processor and Controller. Each of these concepts is defined in the DP Law and will be explained in this guide. There are also FAQs available on the Commissioner's website that may be helpful for quick references to specific topics.

Controllers store Personal Data in relation to Data Subjects for numerous reasons. Personal Data should normally be provided for a specific purpose and not used for any purpose. Personal Data includes all written data, tapes, recordings, photographs, electronic messages, computer-related sources and may be further categorised under the Legislation as Special Category Data, depending upon the nature of the data. The DP Law requires that where data is Processed by a Controller, it must meet certain principles and comply with the stated obligations.

The Controller may appoint a third party to carry out Processing functions on its behalf. This party is known as a "Processor". In circumstances where the Controller appoints a Processor, the Controller remains responsible for the Processing of the Personal Data and for ensuring compliance with the DP Law.

How is the DP Law applicable?

Article 6 of the DP Law states that it is applicable to both Controllers and Processors in the DIFC, as well as such entities outside the DIFC in the context of the Processing conducted as part of stable arrangements, other than on an occasional basis. Stable arrangements comes from the concept in law that a legally binding or recognized agreement or relationship of an existing, valid sort may be enough to require that the principles and objectives of the DP Law are demonstrated in such arrangement. While non-DIFC entities may be subject to the law either directly or indirectly, they are not necessarily required to register or notify operations to the Commissioner other than by way of the relationship with the DIFC-based relevant entity, nor are the required to complete other administrative tasks. They may however be subject to fines, warnings or public reprimand by way of such relationship or arrangements, either directly or indirectly.

What is Personal Data?

Personal Data is any Data relating to an identified natural Person or Identifiable Natural Person.

What is an Identifiable Natural Person?

An Identifiable Natural Person is 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 (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

What is Special Category Data?

Special Category Data is 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 and

including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person. Under this definition, Personal Data is extended to "direct or indirect" data that is sensitive to the Data Subject.
It is important to distinguish Special Category Data from Personal Data as there are different legal obligations for each of these types of information, particularly in relation to Processing.

One of the ways in which Special Category Data can be Processed is by explicit consent of the Data Subject as set out in Article (11)(a). The use of the word "explicit" suggests that the consent of the Data Subject should be absolutely clear. It should cover the specific details of the Processing, the particular type of Personal Data to be Processed (or even the specific information itself), the purpose of the Processing and any special aspects of the Processing which may affect the Data Subject, for example, disclosures which may be made.

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

The definition of Processing is very broad and covers almost any action involving Personal Data.

Who is a Data Subject?
A Data Subject is the individual to whom Personal Data relates.

A Data Subject must be a natural living person. Companies and other corporate and unincorporated bodies, including partnerships, unincorporated associations, governments and states cannot be Data Subjects. Provided the relevant entity is subject to the Law, rights with regard to the Personal Data are available to every Data Subject, regardless of nationality or residence.

Therefore, all the employees in a company located within the DIFC would be categorised as Data Subjects.

Who is a Controller?
A Controller is any person in the DIFC who alone or jointly with others determines the purposes and means of the Processing of Personal Data. A Joint Controller is any Controller that jointly determines the purposes and means of Processing with another Controller.

In the case of a sole trader or partnership an individual may be the Controller. In the case of a company and other corporate and unincorporated bodies, the responsibility for compliance with the Law should rest with an appropriately senior person.

In particular a Controller must ensure that Personal Data is only Processed for "specified, explicit and legitimate purposes". The view of the Commissioner that the determination of the purposes for which Personal Data is to be Processed is a key task which enables a Controller to be able to comply with the Law.

The determination of the purpose and the means by which any Personal Data is, or are to be Processed does not need to be exclusive to one relevant entity. Such determination may be shared with others. It may be shared jointly or in common. For example, a bank with more than one branch may share a central database, but each branch is Processing Personal Data independently of the other branches.

Who is a Processor?
A Processor is any person who Processes Personal Data on behalf of a Controller, and a Sub-processor is appointed by the Processor.

A Processor may be an individual or a body corporate. The former will occur in the case of a sole trader or partnership and the latter will include a company, partnership, unincorporated association, government or state. Irrespective of a Processor being an individual or a body corporate, the Processor has the same responsibilities under the Law.

If a Processor is appointed by the Controller, the latter continues to retain its obligations and responsibilities under the DP Law. In circumstances where this occurs, the Controller should enter into contractual arrangements that reflect its requirements to comply with the Law. The Controller must choose a Processor that can provide sufficient guarantees in respect of the technical security measures and organisational measures governing the Processing to be carried out.

FOR THE PURPOSES OF THIS GUIDANCE, THE TERM "RELEVANT ENTITY" WILL BE USED TO ADDRESS EITHER THE CONTROLLER OR PROCESSOR UNLESS OTHERWISE SPECIFICALLY INDICATED.

Who is a Third Party?
A Third Party is any person authorised to Process Personal Data, other than the:

(a) the Data Subject;
(b) the Controller;
(c) Joint Controller;
(d) the Processor; or
(e) Sub-processor

The expression "Third Party" does not include employees or agents of the Controller or the Processor, these persons are for the purpose of this expression to be interpreted as being part of the relevant entity.

What determines whether "information relates to an identified natural Person or Identifiable Natural Person"?
Potentially, this aspect of the definition of Personal Data may be construed very widely. In the Commissioner's view, whether or not information relates to a particular individual will be a question of fact in each particular case. One element to be taken into account would be whether a relevant entity can form a connection between the information and the individual, and if so, that would amount to Personal Data. Personal Data may not relate solely to one individual as the same Personal Data may relate to two or more people and still be the Personal Data of each of them. For example information concerning a joint

bank account relates to both account holders and therefore is the Personal Data of each account holder and would be protected as such.

How does the Commissioner determine if a natural Person is capable of being "identified"?
A Person must be capable of being identified from the information in the possession of the relevant entity. The Commissioner recognises that a Person may be "identified" without necessarily knowing the name and address of that particular Person. The Commissioner's view is that it is sufficient if the Personal Data is capable of distinguishing a Data Subject from any other Person. For example, in the context of the internet, many e-mail addresses are Personal Data where the e-mail address clearly identifies a particular individual such as the e-mail address. J.Smith@difc.ae is Personal Data. This is because "J. Smith" is an identifiable individual with an electronic address and that address would therefore be categorised as Personal Data.

In the majority of cases, the ability to "identify" a Person will be achieved by knowing the name and address of a Person or having valid identification available.

Can Personal Data be anonymised?
Yes, although rather difficult to truly, properly anonymise Personal Data, a relevant entity may seek to anonymise the Personal Data it is Processing.

In anonymising Personal Data, the relevant entity will be Processing the Personal Data and will therefore still need to comply with the Law until it is finally anonymised.

The Commissioner recognises that the aim of anonymisation is to provide better data protection. However, true anonymisation may be difficult to achieve in practice. Nevertheless, the Commissioner would encourage that, where possible, information relating to a Data Subject, which is not necessary for the particular Processing being undertaken, be stripped from the Personal Data being Processed.

What about expressions of opinion?
Personal Data includes "any information" relating to an individual. Therefore this may include an employer's appraisal or opinion of an employee.

PART 2 OF THE DP LAW: GENERAL REQUIREMENTS - CORE PROVISIONS

Controllers and Processors must ensure that they comply with each of the requirements in respect of Personal Data and the Processing of Personal Data as set out in the DP Law.

In the case of a sole trader or partnership an individual may be a Controller or Processor.

In the case of a company and other corporate and unincorporated bodies, the responsibility for compliance with the Law should rest with an appropriately senior person such as the Chief Executive Officer, General Counsel, Managing Director. However irrespective of which senior person takes responsibility for compliance with the Law, it is the relevant entity that remains responsible at all times under the DP Law.

The relevant entity must retain the Personal Data and the Special Category Data securely and only use that Personal Data in accordance with the DP Law. The relevant entity must ensure that Personal Data is kept up to date and is not retained longer than necessary.

In relation to the transfer of Personal Data, the relevant entity must ensure that Personal Data is only transferred to a jurisdiction outside the DIFC, if that jurisdiction has adequate levels of data protection unless it falls into one of the exemptions set out in the Law. Most importantly, the relevant entity must have systems and procedures in place to ensure that Personal Data is Processed for the purposes or related purposes which the Data Subject expected, unless one of the exemptions outlined in the Law applies.

The relevant entity must notify the Commissioner in relation to the transfer of Personal Data to jurisdictions outside the DIFC that are not aligned with the DP Law.

Operation of the Legislation

When considering the rights and obligations under the Legislation, it is important to remember the wide scope of the definition of "Processing" and, in particular, the fact that the term includes "collection" and "disclosure" of Personal Data.

The core provisions in Article 9(1) may be summarised as follows:

(a) Processed in accordance with Article 10 of the DP Law;
(b) Processed lawfully, fairly and in a transparent manner in relation to a Data Subject;
(c) Processed for specified, explicit and legitimate purposes determined at the time of collection of Personal Data;
(d) Processed in a way that is not incompatible with the purposes described in Article 9(1)(c);
(e) relevant and limited to what is necessary in relation to the purposes described in Article 9(1)(c);
(f) Processed in accordance with the application of Data Subject rights under this Law;
(g) accurate and, where necessary, kept up to date, including via erasure or rectification, without undue delay;
(h) kept in a form that permits identification of a Data Subject for no longer than is necessary for the purposes described in Article 9(1)(c); and
(i) kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

"Processed fairly, lawfully and in a transparent manner"

Fairly means the first and paramount consideration is the consequence of the Processing on the interests of the Data Subject. In assessing fairness, consideration must be given to the purpose and the nature of the Processing. Compliance must be fair in that it must have due regard for the rights and interests of the Data Subject. The Processing requirement of the Law provides an opportunity for the relevant entity to obtain consent from the Data Subject. Alternatively, Processing may be unfair in circumstances where an electronic processing program is itself operating correctly, but results in the unfair use of Personal Data, or where a program is of poor quality and contains errors which mean that it does not operate as the relevant entity intended.

Lawfully means complying with all relevant rules of law, relating to the purpose and ways in which the relevant entity Processes Personal Data. An example of where Personal Data may be unlawfully obtained is where Personal Data is obtained as a result of a breach of confidence or in breach of enforceable contractual agreement.

There are certain areas of law concerning the use of data and the relationship of DIFC Entities with Data Subjects, which may have particular relevance in considering the use of the word "lawfully". These are:

(a) confidentiality arising from the relationship of the relevant entity with the Data Subject; and

(b) legitimate expectation. That is the expectation of the Data Subject as to how the relevant entity will use its Personal Data.

In a transparent manner means that Personal Data is handled on the basis in which it was provided. Most Data Subject's provide it on the basis of trust and on the understanding that it is used only for the purpose for which it was provided. A Data Subject's legitimate expectation as to how its Personal Data will be used is relevant in considering whether or not there has been a breach of this provision.

PLAYBOOK:

A relevant entity must securely keep any Personal Data it collects and Process it fairly and lawfully.

At or before the time Personal Data is collected from a Data Subject, a Controller should take reasonable steps to ensure the Data Subject is aware of:

- the identity of the Controller and how to contact it;
- the fact that the Data Subject is able to gain access to their Personal Data;
- the purposes for which their Personal Data is collected;
- other parties to whom the Controller usually discloses data of that kind; and
- the main consequence for the Data Subject if all or part of the data is not provided.

WHAT ACTION MIGHT I CONSIDER?

Establish an information security policy, review and test IT systems and ensure staff and Third Parties (where possible) are educated about secure practices. They are all part of the technical and organisational measures mentioned in the DP Law.

"Processed for specified, explicit and legitimate purposes determined at the time of collection of Personal Data" or "…in a way that is not incompatible with the purposes described in Article 9(1)(c)."

The DP Law prohibits a relevant entity from Processing, (i.e., collection, storage or disclosure) Personal Data about a Data Subject for a purpose, or related purposes, other than in accordance with the Legislation. In deciding whether any disclosure of Personal Data is compatible with the purpose, or related purposes, for which the Personal Data was obtained, consideration will be given to the purpose, or related purposes, for which the data is intended to be Processed by any person to whom it is disclosed.

In practical terms, if for example a bank collects Personal Data from an individual and that Personal Data was provided for a banking purpose, it may be a contravention of the Law for the bank to transfer the individual's Personal Data to the bank's subsidiary for the use of marketing an insurance product which is not related to the banking activity for which the Personal Data was originally provided.

PLAY BOOK:

A relevant entity should not Process Personal Data unless it is for the purpose it was provided, and should:

- specify the purpose for which Personal Data is being collected;
- ensure that the purpose is lawful;
- ensure that the purpose is made known to the Data Subject;
- ensure that the purpose is known to those for whom and about whom, the Personal Data is being kept; and
- ensure that Personal Data is not collected on the premise that it may come in useful at a later date.

WHAT ACTION MIGHT I CONSIDER?

Think about how to let individuals know about what you would like to do with their data once you collect it. A privacy notice or policy that is publicly accessible or available in simple terms as part of the information provided to an individual setting out the purposes for which data is collected or agreeing specific purposes in a contract or otherwise is good practice.

Consider using examples of other privacy policies from well-known, trustworthy organisations of similar size, type or industry, or have a look at the DIFC privacy policy as a template.

“relevant and limited to what is necessary in relation to the purposes described in Article 9(1)(c).”

In complying with this provision, relevant entities should seek to identify the minimum amount of Personal Data it is required to hold in order to properly fulfill the purpose. This will be a question of fact in each case.

Where a relevant entity holds the Personal Data of several individuals but only requires the Personal Data of a few of those individuals to fulfill the purpose, it is possible that the amount of Personal Data the relevant entity holds is excessive. Any Personal Data held that is not required to fulfill the purpose should be deleted.

It is not acceptable to hold Personal Data on the basis that the Personal Data may be useful in the future without knowing how it will be used. This situation needs to be distinguished from holding Personal Data in the case of a particular foreseeable contingency which may never occur. For example, where an employer holds an employee’s blood group in case of future accident.

Relevant entities should continually monitor compliance with this provision which has obvious links with the other provisions in the DP Law. Changes in circumstances or failure to keep Personal Data up to date may mean that the Personal Data that was originally adequate becomes inadequate. If Personal Data is kept for longer than necessary then it may be both irrelevant and excessive. In most cases, relevant entities should be able to remedy possible breaches of the Legislation by the erasure or addition of particular items of Personal Data.

PLAYBOOK:

The relevant entity should consider the following for all data:

- purpose for which it holds Personal Data;
- number of individuals identified in the Personal Data it holds;
- nature of the Personal Data;
- length of time it holds Personal Data;
- procedure for individuals identified by the Personal Data it holds to obtain access to their Personal Data; and
- the possible consequences for individuals identified by the Personal Data it holds as a result of the way it holds, erases or Processes Personal Data.

WHAT ACTION MIGHT I CONSIDER?

Establish a data retention policy that aligns with the laws to which the entity is subject. Consider as part of an Article 14 privacy compliance policy / program training and internal policies that archive data, provide classifications of the data, and purge it if possible in a way that meets the requirements of being put beyond further use, as set out in Article 22. The more Personal Data your entity keeps, the more it is responsible for and the more likely the damage to data subjects should there be a breach.

"Processed in accordance with the application of Data Subject rights under this Law"

Articles 32 to 40 set out rights that Data Subjects may exercise, which support their fundamental right to privacy and private life. Further detail is provided later in this guidance.

"accurate and, where necessary, kept up to date, including via erasure or rectification, without undue delay"

Personal Data is inaccurate if it is incorrect or misleading as to any fact. A relevant entity would not be in breach of this requirement if:

(a) considering the purposes for which the Personal Data was obtained and Processed, the relevant entity has taken reasonable steps to ensure the accuracy of the Personal Data; and

(b) the Data Subject has notified the relevant entity that it knew its Personal Data was inaccurate and its Personal Data indicates that fact.

It is important to note that by virtue of paragraph (a) above, it is not enough for a relevant entity to say that because the Personal Data was obtained from either the Data Subject or a third party, it had done all that it could reasonably have done to ensure the accuracy of the data at the time. A relevant entity may have to go further and take reasonable steps to ensure the accuracy of the Personal Data itself and mark the Personal Data with any objections. The extent to which such steps are necessary will be a matter of fact in each case and will depend upon the nature of the Personal Data and the consequences of the inaccuracy for the Data Subject.

The second part of the provision which refers to updating Personal Data is only required where "necessary". The purpose for which the Personal Data is held or used will be relevant in deciding whether updating is necessary. For example, if the Personal Data is intended to be used merely as a historical record of a transaction between the relevant entity and the Data Subject, updating would be inappropriate. To change the data so as to bring them up to date would defeat the purpose of maintaining the historical record. However, sometimes it is important for the purpose, that the Personal Data reflect the Data Subject's current circumstances, for example, if the Personal Data is used to decide whether to grant a financial services license. In those cases, either reasonable steps should be taken to ensure that the Personal Data is continually kept up to date, or when the Personal Data is used, consideration should be taken of the fact that the Personal Data may not be up to date.

PLAYBOOK:

The relevant entity will need to consider the following matters:

- is there a record of when the Personal Data it holds was recorded or last updated?
- are all those involved with the collection and Processing of Personal Data, including people to whom it is disclosed, as well as

employees of the relevant entity, aware that the Personal Data may not necessarily be up to date and accurate?

- are steps taken to update the Personal Data, for example, by checking back at intervals with the original source or with the Data Subject? If so, how effective are these steps?

- if the Personal Data is out of date is it likely to cause damage or distress to the Data Subject?

WHAT ACTION MIGHT I CONSIDER?

Have a plan and regular review with all relevant teams about collection methods, disposal and retention methods, and clarify in internal policies and procedures what the entity should do to keep data up to date. If regular outreach to individuals and Third Parties would help, train a team to engage in those actions and maintain a status and risk register as part of the Article 15 Record of Processing Activities.

"kept in a form that permits identification of a Data Subject for no longer than is necessary for the purposes described in Article 9(1)(c)"

If Personal Data has been recorded because of a relationship between the relevant entity and the Data Subject, the need to keep the Personal Data should be considered when the relationship ceases to exist. For example, the Data Subject may be an employee who has left the employment of the relevant entity. The end of this relationship will not necessarily cause the relevant entity to delete all the Data Subject's Personal Data. It may well be necessary to keep some of the Data Subject's Personal Data so that the relevant entity will be able to conserve details of the Data Subject's employment. For example, the provision of references in the future or to enable the employer to provide the relevant information in respect of the Data Subject's pension arrangements. In these circumstances, the Data Subject usually consents to the data being maintained.

Unless there is some reason for a relevant entity to keep Personal Data, Personal Data should be deleted when the possibility of a claim arising no longer exists. The relevant entity cannot retain Personal Data just for the sake of keeping it, unless there is a valid reason to retain the Personal Data.

The relevant entity is under an obligation to continuously consider the value of the Personal Data it has collected and to determine at appropriate stages whether the Personal Data it holds is still necessary for the purpose or purposes for which it was collected.

PLAYBOOK:

The Controller or Processor should ensure:

- that Personal Data that has been Processed is kept in a form which enables the Controller or Processor to determine whether that Personal Data is still required;

- that Personal Data is not kept for longer than necessary given the purpose or related purposes for which it was collected or further Processed;

- maintenance of internal processes and procedures to ensure that the Personal Data is maintained in accordance with the Legislation; and

- that an audit report is conducted on all the Personal Data that is maintained and the type of Personal Data that has been erased in accordance with the requirements of the Legislation.

WHAT ACTION MIGHT I CONSIDER?

In order to comply with this provision, relevant entities must have appropriate processes in place to ensure Personal Data held is reviewed on a regular basis and unnecessary Personal Data held deleted.

Security of Processing

Ensuring that Personal Data is kept securely to protect the rights of Data Subjects is an important feature of the Law. Article 9 of the Law requires that DIFC Entities must take appropriate security measures and must do the following:

(1) implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or other unlawful forms of Processing;

(2) implement such measures to ensure a level of security appropriate to the risk represented by the Processing and the nature of the Personal Data to be protected; and

(3) where Processing is carried out on behalf of the relevant entity, the Controller must choose a Processor that provides sufficient guarantees in respect of the technical security measures and organisational measures governing the Processing to be carried out, and thus ensure compliance with those measures.

There is no specific set of security measures that are required for compliance with the DP Law. Each case will depend upon the circumstances and the business of the Controller or Processor. In considering what is appropriate, the Controller or Processor should consider the impact and harm that might result from, for example, an unauthorised disclosure of the Personal Data, which in itself might depend on the nature of the Personal Data. The relevant entity, therefore, needs to adopt a risk-based approach in determining what measures are appropriate. In delivering a risk-based approach, management and organisational measures are as important as technical ones.

PLAYBOOK:

A relevant entity must take reasonable steps to secure Personal Data and should consider the following:

- the sensitivity of the Personal Data it holds;
- the harm that is likely to result to the individuals about whom the Personal Data relates if there is a breach of security;
- how it stores, Processes and transmits the Personal Data;
- the size of the relevant entity and the level of security that is likely to be required;

WHAT ACTION MIGHT I CONSIDER?

Steps that a relevant entity could take to ensure compliance with Article 14:

- risk assessment – identifying the security risk to Personal Data held by a relevant entity and the consequences of a breach of security;
- security policy – developing a policy that implements measures, practices and procedures to reduce the identified risk to security;
- staff training – train staff and management in security awareness, practices and procedures;
- monitor and review – monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures;
- conducting internal audits to ensure compliance with the Law.

Protecting the security of Personal Data could consist of maintaining the following:

- physical security – by adopting measures to prevent unauthorised entry to premises, systems to detect unauthorised access and secure containers for storing paper-based Personal Data;
- computer and network security – by adopting measures to protect computer systems and networks for storing, Processing and transmitting Personal Data from unauthorised access, modification and disclosure;
- communications security – by protecting communications via data transmission, including e-mail and voice, from interception and preventing unauthorised intrusion into computer networks; and
- personal security – by adopting procedural and personal measures

for limiting access to Personal Data by authorised staff for approved purposes and controls to minimise security risks to a relevant entity's IT systems; and

- destruction of data - taking reasonable steps to ensure proper destruction of both paper and electronic data stored and available on the systems and having appropriate methods for erasing Personal Data.

What are the requirements for "explicit consent"?

The Commissioner is of the view that explicit consent can be conveyed orally or in writing. However, if obtaining consent, then in most circumstances it is recommended that written consent from the Data Subject is obtained. Where consent has been obtained orally, a detailed file note of the relevant details of the consent should be retained.

Further guidance on consent can be found on the Commissioner's website.

General Requirements of Accountability: Articles 14 to 22

Policies, Compliance Program, Design and Default and Preferences

All relevant entities must:

(a) establish a program to demonstrate compliance with the DP Law, the level and detail of which will depend on its scale and resources;

(b) implement appropriate technical and organisational measures to demonstrate that Processing is performed in accordance with the Law;

(c) integrate necessary measures into the Processing that protect a Data Subject's rights by following the principle of "data protection by design and by default, meaning that basic data protection principles are reinforced in the design of the Processing to be undertaken and by default, Personal Data is Processed as necessary to satisfy the specified purposes and in a manner that limits accessibility to the Personal Data by others;

(d) set default privacy preferences on any online services platform that minimize the Personal Data that is Processed in order to deliver or receive the service, allowing the Data Subject to select and easily change preferences; and

(e) implement a written data protection policy that is proportionate to the type of Processing carried out and consistent with the DP Law or alternatively, or adhere to an approved code of conduct or certification scheme.

Notifications to the Commissioner

Controllers or Processors shall register with the Commissioner by filing a notification of Processing operations using the DIFC Client Portal, which shall be kept up to date through annual notifications amended as needed. The DIFC Client Portal will remain the source

for any relevant DIFC registered entity to receive communications, updates and other helpful information generally and as it regards data protection. The DIFC may also use the information provided in the DIFC Client Portal (or through other means) to communicate directly through email, text message or via app messaging. Please see the DIFC Terms of Use and DIFC Online Data Protection Policy for further information about how the DIFC or the Commissioner's Office may communicate with you.

Whenever such notifications are received by the Commissioner the details will be set out on the DIFC Public Register in order to act in part as a notification to any Data Subject that a relevant entity may be Processing his or her personal data. It is a form of accountability and ensures up to date information about the relevant entity is available in order to assert any rights.

Notification fees are set out here.

Ultimately, the format of the notification aligns directly with the format of the DP Law and this guidance. Once completed, if printed out or saved as a PDF, the notification may serve as a skeleton outline or guide for establishing the compliance requirements set out in the sub-section above.

If you have any questions about the use of the DIFC Client Portal please contact the Portal helpdesk.

Further guidance on notifications is available on the Commissioner's website.

Records of Processing Activities

Controllers and Processors must maintain written records of Processing activities (ROPA) for which it is responsible or carrying out as instructed. The ROPA must contain information that makes clear where it is based, who is responsible for data protection activities, such as a data protection officer, who receives the information it collects and / or Processes, transfers of such data and to where, technical and organizational measures that are applied to the Processing and any time limits for erasure of such data. Currently there are no Regulations regarding the form or process for a ROPA. This will depend largely on the policies and Processing activities that make sense for the relevant entity.

Designation of the DPO

A Data Protection Officer independently oversees relevant data protection operations within a Controller or Processor's business. It is only mandatory to appoint a DPO in specific instances:

(a) as a DIFC Body (i.e., the DFSA or the Courts);
(b) where High Risk Processing Activities are undertaken (please see the Commissioner's guidance for understanding this concept); or
(c) where the Commissioner requires that a DPO is designated.

Otherwise, if no DPO is appointed the relevant entity must clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations under this Law, or any other applicable data protection law, within its organisation and be able to provide details of the persons with such responsibility to the Commissioner upon request.

The DPO may already be appointed within a group of companies, and must only be resident in the UAE unless he is employed within such group and provides such function on an international basis.

The DPO must have sufficient expertise, independence and resources to effectively and objectively perform his duties. The DPO must also be prepared to work with the Commissioner and his office in order to discuss and provide relevant information in a transparent and cooperative way.

Compliance with the DP Law and continuous monitoring is a key task of the DPO. Providing advice and feedback on the provisions of the DP Law in a professional, clear and informative manner is of utmost important. The DPO will conduct the **Controller Annual Assessment** under Article 19 and any necessary data protection impact assessments (DPIA) as set out in Article 20.

DPIAs

A data protection impact assessment shall contain at least:

(a) a systematic description of the foreseen Processing operations and the purpose(s) of the Processing, including, where applicable, the legitimate interest pursued by a Controller;

(b) an assessment of the necessity and proportionality of the Processing operations in relation to the purpose(s);

(c) identification and consideration of the lawful basis for the Processing, including:

    (i) where legitimate interests are the basis for Processing, an analysis and explanation of why a Controller believes the interests or rights of a Data Subject do not override its interests; and

    (ii) where consent is the basis for Processing, validation that such consent is validly obtained, consideration of the impact of the withdrawal of consent to such

(d) an assessment of the risks to the rights of Data Subjects; and

(e) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Law, taking into account the rights and legitimate interests of Data Subjects and other concerned persons.

The Commissioner may publish information that will aid in DPIAs and Annual Assessments, including what is considered High Risk Processing. Please check back to the Commissioner's page on the DIFC website for further information and templates. The Commissioner may also publish a list of the types or categories of Processing operations for which no data protection impact assessment is required.

Article 20 of the DP Law provides further details about what constitutes a valid DPIA.

Please note regarding Annual Assessments and DPIAs that the Commissioner has posted templates on the Forms and Fees section of the Commissioner's page of the DIFC website, accompanied within the template by details of how to carry out these assessments out and against what metrics they should be measured.

Prior Consultation

Article 21 contains provisions for the concept of prior consultation with the Commissioner's Office in the case of certain types of Processing activities. Controllers must consult with the Commissioner on Processing that is particularly high risk despite taking any mitigating measures to reduce such risk. In other cases, Controllers may consult with the Commissioner in any case, and may carry out Processing before or during consultation as long as it is unlikely to negatively impact the Data Subjects whose Personal Data is being Processed.

Cessation of Processing

Subject to certain conditions set out in Article 22(4), Article 22(1) sets out the requirements to be complied with when Processing ceases. Where the basis for Processing changes, ceases to exist or a Controller is required to cease Processing due to the exercise of a Data Subject's rights, the Controller shall ensure that all Personal Data, including Personal Data held by Processors is:

(a) securely and permanently deleted;

(b) anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released;

(c) pseudonymised;

(d) securely encrypted; or

Where a Controller is unable to ensure that Personal Data is securely and permanently deleted, anonymised, pseudonynmised or securely encrypted, the Personal Data must be archived in a manner that ensures the data is put beyond further use.

PART 3 OF THE DP LAW: OBLIGATIONS OF CONTROLLERS AND PROCESSORS

Articles 23 to 25 cover what contractual and other obligations that must be complied with by Controllers (including Joint or co-Controllers) and Processors (including Sub-processors). Fundamentally, all entities must have written agreements in place that make clear all relevant aspects of the Processing that is taking place, as well as any instructions, commitments to provide accountability and confidentiality, to secure the Personal Data being Processed, to comply with requests for information or audits to the extent required by Applicable Laws, and generally to comply with data protection principles as set out in the DP Law, Regulations and any associated guidance.

PART 4 OF THE DP LAW: DATA EXPORT AND SHARING

Article 26 of the Law states that a transfer of Personal Data to a Recipient located in a jurisdiction outside the DIFC may take place only if an adequate level of protection for that Personal Data is ensured by laws and rules that are applicable to the Recipient, including with respect to onward transfers of Personal Data; or where it takes place in accordance with Article 27.

Under the Law, there are strict requirements for the transfer of Personal Data outside the jurisdiction of the DIFC.

What is an adequate level of protection?

Article 26(1)(a) of the DP Law makes reference to an adequate level of protection in Third Country. It requires the assessment of all the circumstances surrounding a Personal Data transfer, which includes:

(a) the nature of the Personal Data;

(b) the purpose and duration of the proposed Processing operation or operations;

(c) if the Personal Data does not emanate from the DIFC, the country of origin and the country of destination of the Personal Data; and

(d) any relevant laws to which the Recipient is subject, including professional rules and security measures.

Under Article 27 of the DP Law, Personal Data may be transferred outside the jurisdiction of the DIFC in the absence of an adequate level of protection in the other jurisdiction, if a Data Subject has provided its "explicit" consent. This means that there must be some active communication between the parties. Though a Data Subject may give "explicit" consent, relevant entities cannot infer consent from non-response to a communication, for example from a customer's failure to return or respond to a leaflet. The adequacy of any consent or purported consent must be evaluated. For example, consent obtained under duress or on the basis of misleading information will not be a valid.

PLAYBOOK:

Before Personal Data is transferred outside the DIFC the relevant entity should consider the following matters:

- has the Data Subject appropriate consent to the proposed transfer?
- is the transfer necessary for the performance of a contract, or for the conclusion or performance of a contract that is in the interest of a Data Subject between a Controller and a Third Party?
- is the transfer necessary or legally required for reasons of Substantial Public Interest (see definition in Schedule 2 of the DP Law), or for the establishment, exercise or defence of legal claims?
- is the transfer necessary or legally required in the interests of the DIFC, including

in the interests of the DIFC Bodies relating to the proper discharge of their functions?

- is the transfer necessary to protect the vital interests of the Data Subject?
- is the transfer intended to provide information to the public which is open to consultation such as a register or for viewing by the general public?
- is the transfer necessary for compliance with any legal obligation?
- is the transfer necessary to uphold the legitimate interests of the relevant entity recognised in the international financial market?
- is the transfer necessary to comply with auditing, accounting or anti money laundering obligations that apply to a relevant entity?

WHAT ACTION MIGHT I CONSIDER?

Take time to review the above as well as Articles 26 and 27. Set out a consistent policy or approach to ensuring secure transfers to non-adequate jurisdictions including to other parts of your business that are onshore in the UAE. Choose an appropriate transfer mechanism in accordance with Article 27. If you the standard data protection clauses (Controller to Controller or Controller to Processor) are chosen, review them regularly, ensure they are completed properly and executed.

Standard Data Protection Clauses

The Commissioner, in accordance with Article 27(2)(c) of the DP Law, has provided a set of standard clauses to be applied to contractual or other arrangements that require the transfer of Personal Data outside of the DIFC. They are available on the Forms and Fees section of the Commissioner's Page of the DIFC website.

The standard clauses may not be altered other than to complete basic information or provide additional commercial requirements. If any alteration to the standard clauses is contemplated by the relevant entity utilizing them, the Commissioner should be consulted first and such alterations agreed in writing. The Commissioner reserves the right to reject at his own discretion any such application for alterations.

Any existing agreements that require transfers out of the DIFC but are not in compliance with the DP Law should be amended within a reasonable time period if not at least by the next renewal date of such agreement. If the agreement renewal date is at a point in the future such that not amending the agreement will negatively impact the rights of the Data Subjects concerned with the Processing, it is recommended that the agreement is amended forthwith.

Data Sharing

It is common for government organizations or authorities to request data, including Personal Data, on demand for a variety of positive purposes. While the Commissioner encourages such sharing, the organization receiving such request still needs to consider what controls should be in place to govern the sharing and ensure that all parties involved will apply them. If the organisation deems a request too broad, it may ask for specificity or request appropriate, written binding assurances that the data will be ethically and responsibly managed.

PLAYBOOK:
Before Personal Data is shared in response to a request for information the relevant entity should consider:

- Is all of the information in the request necessary to share?
- Is it subject to another law or regulation, thereby limiting the decision about whether to share or not, i.e., for the prevention of crime or for reasons that could save an individual's life or health?

WHAT ACTION MIGHT I CONSIDER?

Article 28 contains this relatively new but important concept, and allows for the creation of policies regarding sharing Personal Data with government entities. Please contact the Commissioner's Office for assistance in this regard and check the Commissioner's website to examples of such policies.

PART 5 OF THE DP LAW: INFORMATION PROVISION

Articles 29, 30 and 31 of the DP Law set out the expectations and requirements for processing notices and privacy policies of Controllers and Processors. Such information provision supports the notion of accountability and transparency. Notices may be provided in writing or orally, but the latter depends on the circumstances, i.e., that the identity of the Data Subject has been verified. Such policies must be written in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Generally, a Data Subject is entitled to know what data is collected, how it is Processed, what specific purposes it may be used for (i.e., direct marketing; please see associated guidance), contact details of the DPO, their rights including the ability to unsubscribe or withdraw consent to Processing the Personal Data, and any other similar information that may assist them in dealing with an organization that is Processing his information. This information must be provided within one (1) month of obtaining the data. So for example, if Personal Data is collected or used in a way or for a purpose not originally set out in the notice, the notice should be updated within that time period so that the Data Subject has all up to date information. It may also be notified no later than the first communication with the Data Subject or if a disclosure of information is requested, no later than the time when it is first disclosed. There are certain limitations for such information provision including where obligations exist under Applicable Laws. Please review Articles 29 and 30 for further information.

PART 6 OF THE DP LAW: RIGHTS OF DATA SUBJECTS

Protection of rights

The DP Law gives rights to Data Subjects in relation to their Personal Data and Special Category Data held by others in Articles 32 to 40. These include the right:

(a) to withdraw consent at any time and for any reason;

(b) to access Personal Data;

(c) to take action to rectify, restrict, erase or destroy inaccurate data;

(d) to object to the Processing of Personal Data at any time on reasonable grounds relating to the individual's situation.

(e) to be informed before Personal Data is disclosed for the first time to third parties or used on their behalf or to object to disclosure to third parties or in relation to direct marketing;

(f) for the individual to lodge a claim, make a complaint and request mediation;

(g) for portability of his or her Personal Data between Controllers;

(h) to object to any decision based solely on automated Processing, including Profiling, which produces legal consequences concerning him or other seriously impactful consequences and to require such decision to be reviewed manually;

(i) to non-discrimination where the Data Subject exercises any such rights; and

(j) to have available at least two (2) methods of contact the Controller to exercise such rights.

Key rights of Data Subjects

A Data Subject has certain rights provided for under the Law in relation to access to, rectification, objection and disclosure of Personal Data. Additional extensive guidance on this subject is available on the Commissioner's guidance page of the DIFC website.

Controllers will need to take reasonable steps to confirm the accuracy, completeness and currency of the Personal Data it holds at the time they collect, use or disclose that Personal Data. Controllers will be obliged to correct or erase Personal Data they hold should the Data Subject to whom the Personal Data relates, establish on its own review, that it is not accurate, complete or up to date.

If a Controller does not adhere to the request of a Data Subject to correct or erase its Personal Data, Article 59 of the DP Law allows the Commissioner to issue a direction to the Controller requiring it to comply in accordance with the terms of the Commissioner's direction, among other remedies.

PLAYBOOK:

Controllers should focus on areas where inaccurate, incomplete or out of date Personal Data is most likely to have a detrimental effect on individuals it relates to. What are reasonable steps will vary depending upon the circumstances. Controllers should consider the following matters:

- how likely is it that the Personal Data it holds is complete, accurate and up to date;
- whether the kind of Personal Data it holds changes over time;
- how recently it collected the Personal Data;
- how reliable the Personal Data is likely to be;
- who provided the Personal Data; and
- what it uses the Personal Data for.

WHAT ACTION MIGHT I CONSIDER?

If a relevant entity uses Personal Data soon after it is collected from a Data Subject, it may not need to check it. If it collects the Personal Data from someone else, there may be a greater need for the relevant entity to take appropriate action to confirm that it is accurate, complete and up to date.

Right of subject access

Data Subjects are entitled to be told whether they or someone else on their behalf is Processing their Personal Data. If so, Data Subjects should be given a description of:

(a) their Personal Data;

(b) the purposes for which their Personal Data is being Processed; and

(c) Recipients or proposed Recipients of their Personal Data.

A Data Subject is also entitled to receive in an intelligible form, all the information which forms that individual's Personal Data. This information must be supplied in a permanent form by way of a copy, except where the supply of that copy in permanent form is not possible or would involve disproportionate effort, or the Data Subject agrees otherwise.

If any of the information in the copy is not intelligible without explanation, for example, where the relevant entity holds information in code form which cannot be understood without the key to the code, the Data Subject should be given an explanation of that information, and, subject to third party information referred to below, any information as to the source of that data.

Where a Data Subject makes the request under Article 33 of the DP Law, the relevant entity shall comply with the request within one (1) month.

Right to prevent Processing for the purpose of direct marketing

A Data Subject is entitled by written notice, to require a relevant entity to cease, or not to begin, Processing their Personal Data for the purpose of direct marketing. When a relevant entity receives such a notice it must comply as soon as it can. There are no exceptions to this. The Data Subject may lodge a complaint and apply for mediation under Article 60 of the Law if the relevant entity fails to comply.

The Commissioner regards the term "direct marketing" as covering a wide range of activities which will apply not just to the offer for sale of good or services but also to the promotion of a relevant entity's aims and ideals. This would include a charity making an appeal for funds or support. This would also include uninvited telesales calls and uninvited telemarketing facsimile and electronic messages.

Further guidance on marketing and web scraping is available on the Commissioner's website.

PART 7 OF THE DP LAW: PERSONAL DATA BREACHES

Personal data breaches may be required to be notified to either the Commissioner and / or the relevant Data Subject(s), in the latter case where the breach is likely to result in a high risk to the security or rights of a Data Subject. There is no specific time period within which to notify the breach, only that it should be made without undue delay after becoming aware of a breach. Further guidance is available on security breach notification.

PLAYBOOK:

Controllers and Processors should consider the following matters:

- What are the biggest areas for security breach or unauthorised data access or loss?
- Are physical security measures considered in IS policies?
- How well and often are the staff trained about breaches, reporting, and incident management?
- Is there an incident management policy?

WHAT ACTION MIGHT I CONSIDER?

Controllers and Processors are both responsible for breaches and breach reporting. As such, consider adopting an incident management policy, with a clear incident classification, levels of priority, reporting requirements about who to notify and when, as time will be of the essence.

PARTS 8, 9 AND 10 OF THE DP LAW: COMMISSIONER'S POWERS AND APPLICABLE REMEDIES

The Commissioner's powers

The DP Law provides the Commissioner with powers to mediate and to give directions where the rights of a Data Subject have been adversely affected or where there has been a contravention of the Law. He may investigate and conduct inspections, initiate proceedings or claims for compensation on behalf of a Data Subject or for other reasons set out in the DP Law, prepare Regulations for Board approval, and do anything else reasonably necessary to perform his functions. The Commissioner must remain independent and impartial, and will not accept instructions from another party.

The following will focus on certain specific provisions of the Commissioner's powers and functions as they relate to Data Subjects' rights.

Application to the Court and Compensation

Any Controller or Processor who is found to contravene this Law or a direction of the Commissioner may appeal to the Court against the finding within thirty (30) days. Likewise, a Data Subject who disagrees with a finding by the Commissioner of contravention of the Law or of no contravention of the Law may appeal against the finding to the Court within thirty (30) days. A Data Subject may be entitled to compensation for any damage that he may suffer by reason of any contravention by a relevant entity of any requirements of the Law or the Regulations.

Mediation

Mediation is dealt with in Article 60 of the DP Law. Mediation commences with receipt of a complaint by the Commissioner from an affected Data Subject. It may be lodged with the Commissioner when the Data Subject contends that there has been a contravention of the Law or an alleged breach of his rights under the Law.

The Commissioner is not required to undertake a mediation role in respect of every claim lodged. Article 60(3) of the DP Law specifically indicates that the Commissioner "may" mediate between the relevant parties. Accordingly an assessment process is used to determine what matters ought to be the subject of mediation.

Accordingly, a complaint or contention of contravention of the law lodged with the Commissioner will be assessed and he may issue a recommendation as to whether mediation should occur. This information is disseminated to the Data Subject and if applicable, to the relevant entity.

The method of mediation is not prescribed. Section 6 of the Regulations simply provides that the Commissioner should follow such practices and procedures that will lead to the most timely, fair and effective resolution of the claim. Accordingly, the actual method of mediation will be determined by the facts of each matter, but the mediation will be in accordance with international best practice principles. In most cases, the Director of Data Protection or other appointed, competent DIFC representative will be the mediator or may appoint another person to mediate, as appropriate.

Directions

Under Article 59 of the Law, if the Commissioner is satisfied that a relevant entity has contravened or is contravening the Legislation, the Commissioner may issue a direction to the relevant entity requiring it to:

(a) do or refrain from doing any act or thing within such time as may be specified in the direction; and/or

(b) 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.

The direction is issued by the Commissioner of the DIFC and must contain a statement of the contravention of the Legislation. The relevant entity may seek a review of the decision by the DIFC Court.

When the Commissioner considers that the relevant entity has failed to comply with the direction, he may apply to the Court for one (1) or more of the following orders:

(a) an order directing the Controller or Processor or officer to comply with the direction or any provision of the Law or the Regulations or of any Applicable Law administered by the Commissioner relevant to the issue of the direction;

(b) an order directing the Controller or Processor or officer to pay any costs incurred by the Commissioner or other person relating to the issue of the Commissioner's direction or the contravention of such Law, Regulations or Applicable Law relevant to the issue of the direction; or

(c) any other order that the Court considers appropriate.

The Commissioner's directions are subject to review by submitting a request to review the direction within fourteen (14) days of receiving it. The Commissioner may receive further submissions and amend or discontinue the direction. He may also issue warnings where Processing operations are likely to infringe the DP Law or issue public reprimands where processing operations have infringed the DP Law.

Imposition of Fines

The Commissioner may impose both administrative fines and general fines under Article 62.

An administrative fine relates mainly to a contravention of the DP Law as set out in Schedule 2 of the DP Law. These are things like failure to notify, to keep records of Processing operations, appointment of a DPO where required and so on.

A general fine may be imposed for a contravention or action that is in his view considered serious and requires further penalties due to the actual harm caused to any relevant Data Subject. There is no monetary limitation on these types of fines.

Please see additional guidance on fines and sanctions on the Commissioner's guidance page.

Powers to make rules about exemptions

Article 65(1) of the Law gives the DIFCA Board of Directors the power to make Regulations exempting Controllers from compliance with the Law or any parts of the Law.