DIFC

INDIVIDUALS' RIGHTS TO ACCESS & CONTROL PERSONAL DATA PROCESSING

Commissioner of Data Protection

DIFC

CONTENTS

1 Introduction

Understanding Individuals' Rights in the DIFC

The Dubai International Financial Centre and/or its affiliates and entities (collectively "DIFC", "DIFCA") values individuals' security and privacy. DIFC has its own Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law"), and may for certain types of Personal Data processing also apply the laws from other jurisdictions.

Under the DP Law and others like it, individuals ("requestor", "individual", or the combinations or plural of these terms) whose Personal Data is collected and processed have fundamental rights to know about such activities. The DP Law ensures that any individuals have the right to access, rectification, erasure or restricting of the Personal Data that a DIFC registered entity processes about them, if any. Individuals also have the right to object to such processing, or to ask that it be handled manually or given options for portability. The following information addresses how an individual may exercise these rights and sets out guidance for DIFC registered entities about how to respond as set out primarily in Part 6 of the DP Law.

The defined terms used herein have the same meaning as the defined terms in the DP Law.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the DIFC Commissioner of Data Protection (the **Commissioner**) either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

2. Scope

Due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance should be read in conjunction with those existing UK and EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. 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.*

3. Subject Access Requests

Subject Access Rights Explained

The right to access Personal Data is often referred to as a Subject Access Request (an "**SAR**"). Generally, Controllers that hold or process Personal Data about an individual must confirm whether or not Personal Data concerning him or her are being processed, and, where that is the case, the Controller must give the individual access to the Personal Data, with very few and limited exceptions.

Submitting a SAR

A SAR must normally be in writing, but there is no specific format required. What is important is for both parties, the requestor and the Controller, to understand the request in order to respond accordingly. To this end, a responding entity may be required to communicate with the individual to clarify and potentially refine the scope of the SAR response, particularly when a broad quantity of information may be available.

Each SAR is different, and must be responded to on a case by case basis. Steps that may be taken in order to appropriately respond to a SAR include:

- *Authenticate individuals submitting SARs before handing over any data*: A responding entity may request additional information to authenticate your identity when required. Authentication is also a valid security safeguard against providing Personal Data to the wrong person, particularly in the context of online services and online identifiers. If identity of the requestor is unclear, it may impact when the response timing window of one (1) month begins.[1]

- *Refine / Clarify the request, Response time:* A responding entity may ask questions to get a better understanding of the universe of data requested and will indicate potential technological or other issues in advance, especially where a request is particularly complex or unclear. This is to ensure that the responding entity that is the recipient of a SAR provides a response that is reasonably appropriate, useful and informational, and to provide a fair basis and reasonable

[1] *Please note that the one month period may be possible to extend, in accordance with the DP Law Article 33(7) and (12). Please see below for further information.*

estimate of response timing requirements, so they are not inadvertently put in a situation of contravening the DP Law. **Responding to the SAR is only required once such information is received and clear to all parties involved**.[2] Please see additional information on **Response Time** set out in detail below.

- *Searching for Personal Data requested*: A responding entity will use appropriate measures to exhaust its search for the Personal Data that has been requested, but should notify the individual of whether the search will entail disproportionate measures and any next steps to resolve the issue.

- *Format and Delivery:* The DP Law requires that the response must be made in an intelligible form. A responding entity should agree the format of the response with the individual requestor in advance if possible. Also, before supplying any information in response to a SAR, please check that the individual's postal or email address or any other contact information to which the data is to be sent is correct.

Data to be Provided in Response

"Personal Data" can be interpreted very broadly, and may include identifiers – that data which make someone "identifiable" – such as identification numbers, location data, and "online identifiers."

Additionally, Individuals are entitled to be:

- told whether any Personal Data is being processed;
- given a description of the Personal Data, the reasons it is being processed, and whether it will be given to any other organizations or people;
- given a copy of the Personal Data;
- given details of the source of the data (where this is available and disclosable)
- given information about the right to complain to the Commissioner and / or rights to remedies set out in Parts 9 and 10 of the DP Law

Potential Exclusions, Limitations and Exemptions

[2] *Please note that the one month period may be possible to extend, in accordance with Article 33(7) of the DP Law. Please see below for further information.*

A responding entity may reserve the right to exclude data that does not qualify as Personal Data or may not be appropriately responsive to the SAR. For example, it may exclude anonymous data, or notations that are purely internal to its systems, or other information that may not be appropriate to disclose for other valid legal reasons.

Where third party or unrelated data is included in the data set but is not legally required to be provided, it may be redacted or excluded from the data set as appropriate unless the third party has consented to providing their data. However, even if the third party has not consented, it may still be reasonable to include their Personal Data in the SAR response where disclosure is reasonable under the circumstances. Please document your assessment of why such third party Personal Data is included, to demonstrate the decision-making and risk mitigation factors that went into the response contents.

Exemptions and restrictions to providing certain data may apply as well, depending on the circumstances. Any withholding of data due to an exemption or restriction should first be approved by a Data Protection Officer (where applicable) or other suitably qualified person. Where any redaction of information is permitted on whatever basis, the SAR response must clearly and fully explain, to the extent practical, the fact that information has been withheld and the reasons why, as well as the right to complain or appeal.

Any exemptions or limitations on access rights, including those applied by a DIFC Body, must be recorded on an exemption register setting out reasons for use of the exemptions, and made available to inspection by the Commissioner upon request[3]. The Commissioner may at any time request additional information or conduct an investigation, to determine whether the use of the variation or exemption was validly applied. The Commissioner's determination, after considering representations from all persons affected by the request, is final and conclusive, subject to a validly lodged appeal under Article 63(1). A Controller that contravenes the DP Law by invalidly relying on an exemption or limitation shall be subject to the remedies, liabilities and sanctions set out in Part 9 of the DP Law. Please review guidance on fines and other sanctions available on the DIFC DP website.

Response Time

[3] *Please see DP Law Article 33(8) to (11).*

In accordance with the DP Law, the response to the SAR must be provided within one (1) month of the request, subject to any other applicable conditions set out in the relevant provisions of the DP Law. For example, in certain circumstances, it may take a considerable amount of time and / or cost to properly search for the Personal Data requested.

In these cases, a responding entity must continue to communicate with the individual requestor about any timing issues and potential resolutions. A further two (2) months to address particularly complex requests may be assessed as necessary by the responding entity, to be determined on a case by case basis and to be communicated to the individual requestor citing reasons for the delay.

Finally, to summarise the concepts set out above regarding clarification of the SAR and its impact on response time, please recall that identity, clarification of scope (for example due to complexity, broadness of the request, etc.), or other valid factors may affect when, if at all, the response period begins. The fact that a request involves a large amount of data or a potentially vast span of time *does not in and of itself* mean that the request is complex, even where capacity to prepare a response may be limited. This will depend on the size of the entity and available resources, but does not necessarily contribute to the assessment to request a longer response period or starting time for the response. Each such case must be determined individually, based on reasonable, objective factors, in addition to the other steps it may take to assure proper compliance with SAR requirements under the DP Law. For example, additional resources may be necessary where it is unreasonable to extend or delay the start of the response period. *In all cases, regular, transparent communication with the requestor wherever possible will only aid in complying with the DP Law and supporting the exercise of individual's rights to access their data.*

Please consider completing the Request Response assessment tool for further support in making these important initial decisions when responding to an access or other rights-related request.

Fees for SARs

The SAR response should be provided free of charge unless the request results in high administrative costs or the individual requestor asks for additional copies of the documentation provided. If such costs are likely to be or have been incurred, a determination of an appropriate fee may be made and communicated to the individual requestor.

Special Matters

Employee SARs

Human Resources handle many SARs from current employees, job applicants and former employees. Certain issues routinely arise when responding to them, however, which include:

(i) providing for additional time when requests may span a vast amount of time or are rather complex;
(ii) making clear what amounts to a request which is manifestly excessive; and
(iii) appropriate fees for complex, excessive, unfounded or repeat requests.

To be sure, the following specific issues may cut across all SARs, and the guidance below should be read in light of *any* situation, not only Employee SARs. It is in this context that these issues tend to show themselves most often, however, so they are laid out in this section for efficiency's sake.

(i) Additional time

As generally noted above, the fact that a request involves a large amount of data or a potentially vast span of time does not in and of itself mean that the request is complex, and much will depend on the size of the employing entity and available resources. Each such case must be determined individually, based on reasonable, objective factors, in addition to the other steps it may take to assure proper compliance with SAR requirements under the DP Law.

An employer may, where they are seeking to clarify the scope of a SAR with the employee, perhaps because it is too broad or ambiguous, the response time frame will start accordingly once the parties reach agreement over exactly what it is the employee is looking for, where possible. In theory, this outcome can be quite reasonably sorted. In practice, due to various circumstances including the conditions of the departure of an

employee, or management complaints, for example, which most commonly give rise to SARs, a reasonable scope-clarifying outcome may not be achieved. As such, all best, good faith efforts are undertaken to remain as fair and amicable as possible in such situations so that the SAR may be dealt with efficiently and without undue frustration. Where this is not possible, the responding entity should unilaterally be overly inclusive to the extent legally possible, accounting for third parties' privacy rights and other permitted non-disclosure exemptions.

Employers are always required to comply with the obligation to provide a response to a SAR of appropriate form, substance and type, in line with the requirements set out in the DP Law. However, individual requestors should also consider the reasonableness of their request, and how cooperative they are willing to be in order to clarify and agree the scope of their request. Where it is clear that an employer has made best efforts to reach out, clarify, communicate and otherwise undertake a fair approach to the SAR response, what may be objectively considered as unreasonable behavior by the employee may leave the employer with little other choice but to unilaterally decide that the response may be just as broad as the request, and taking into consideration in making this assessment the size of the organisation and availability of resources.

Furthermore, while motive for the request is not generally a factor in the responding entity's decision about whether to respond and the substance of the response, the individual making the SAR should examine his or her requirements carefully and take a more appropriate course for disclosure where it makes sense to do so, including compelling information through a obtaining a court order or the like. Provided the claim is valid and likely to be accepted by the relevant court[4], often information will be more complete and all-encompassing through this or another viable method, because while a response is required, there are several exceptions and exemptions that a responding entity may apply. When this occurs, complaints about the completeness of the response often result, regardless of good faith efforts of the responding entity. Complaints then take additional time and effort to resolve while another course of action for a request may be a more efficient for the requesting individual.

(ii) Manifestly Unfounded / Excessive

[4] *Please note that not all claims will be accepted by the relevant judicial authorities, and seeking legal advice is the most appropriate way to determine the best course of action if you believe you have been harmed in some way. Neither the Commissioner's Office, the intended recipient of the SAR, nor the courts are in a position to provide this advice.*

Please note that the responding entity unilaterally deeming an individual as "uncooperative" is separate and apart from deeming an SAR "manifestly unfounded or excessive", and the motive for making the SAR should continue to not be a factor in determining how or when to respond to a SAR. The "manifestly unfounded or excessive" exceptions factor into a SAR response in only a few, fairly narrow circumstances. If for example the SAR is clearly being used by the individual as a bargaining chip or an inducement to a settlement of some kind (whether financial or otherwise), it may, depending on the case by case circumstances, be reasonable to conclude that it is manifestly unfounded. Generally, though, collateral purposes, often referred to as "fishing expeditions", or actions taken as a form of pressure on an employer in a negotiation, are not necessarily enough to refuse or limit a SAR response. These exceptions should be very rarely applied in rather obvious circumstances, and any assessments of this nature should be very carefully documented.

(iii) Appropriate Fees for Complex, Excessive, Unfounded or Repetitive SARs

Guidance around fees follows a similar methodology as above. Individual SARs will require different resources, and must be determined on this basis. Avoiding charging a fee is always the best option, and in narrow circumstance should a fee be charged. If is agreed that a fee should be charged to respond to the SAR, it should be nominal at most. More than 1000 AED is unlikely to be an acceptable amount to charge for even a substantial SAR response, for example.

The monetary and resourcing risks associated with responding to a SAR may be mitigated by providing fair, well-documented, clear internal and external policies, applied on a consistent basis, and regular curating of employee data to ensure it is readily accessible on an on-going basis. Having consistent policies and checklists in place, including those addressing SAR response procedures, data retention, as well as implementing IT systems and asset or other registers for quick, accurate accessibility will very likely make it easier to respond to a SAR, with more accuracy and substance and without unnecessarily spending time and resources.

Case Study in Employee SARs:

Recently, employee SARs have come under review. The main issue is determining whether an employer responding to and SAR could refuse to provide access to all the contents of a former employee's work email account.

In one such situation, a responding employer provided the former employee with his personnel file, email correspondence which contained personal information about him, as well as other material which contained personal information, but did not provide emails from his closed work email account. The reasoning of the employer was that emails sent in connection with performing work functions could not be considered as “Personal Data”.

Conceptually, the personal information in work emails relates to the employee's function in his or her position with the employer. Emails sent containing personal information about the employee, over and above material relating solely to the performance of his or her work functions, may be an exception, however.

The employer was entitled to refuse sharing work emails in the SAR response because the request was too extensive. Further, it was concluded that email accounts are not themselves IT systems intended to process information about employees.

The employer making a good faith effort to enter into a dialogue with the former employee on how the employer could comply with the request in another way was a positive step, and logically one may conclude that the former employee’s cooperation in this dialogue would be seen as a positive step as well, to the extent he or she can remain professional, courteous and objective about a situation that may often be fraught with emotion. In short, cool heads prevail and in such situations, the SAR response will serve the purpose intended by the DP Law.

Thus, when requests are made to DIFC employer-entities that must respond to an employee’s SAR, they should consider the following in their assessment of whether emails from a work account will be deemed excessive or not containing Personal Data:

- if the entity has a clear work email acceptable use policy on use (or not) of work email for personal purposes, citing unambiguously for example that work email is a digital asset of the employer and use for personal purposes is undertaken at the employee’s own risk, in addition to any other necessary provisos and notices;

- if the policy permits use of work email accounts for purely personal use, that the individual may forgo his or her rights to request any and all work emails in a SAR.

Personal use would logically be construed as communication between the individual and an email recipient for a complete non-work related purpose, i.e., planning a holiday, sending a message of any nature to a friend or family member, making a reservation for non-work activities, and similar non-work matters.

- With appropriate training, as well as notice (as above) to the employees, supervision and enforcement of the work email acceptable use policy, it may be appropriate for an employer to consider access to closed work email accounts as out of scope for an SAR, unless they are willing to apply the resources required to sort through the close work email account.

Any risks that may result in overriding the interests or rights of the individual employee, and associated negative consequences of removing work email account data from the scope of a SAR response, should be considered in a data privacy impact assessment, documented, communicated to the individual in the initial scoping exercise or at the latest in the response itself, and an opportunity to appeal the decision must be provided at any point to the individual.

4. Rectification, Erasure, Objection and Portability

Rights explained

Articles 33 to 37 of the DP Law provide for additional individual rights regarding how Personal Data is managed by a Controller. These rights primarily deal with the data protection principle that Personal Data held and handled by a Controller must be accurate and up to date, as well as processed in a timely manner. Many of the actions and specifics are similar to that of an SAR, as outlined below.

Rectification

Rectification is the right of individuals to have inaccurate Personal Data rectified, or completed if it is incomplete. Best practice suggests a responding entity:

- Verify the accuracy of data by whatever factual means available, including discussions with and collecting data from individuals;
- If the data is linked to an opinion, determine whether the data is indeed inaccurate and needs to be rectified;
- While the above is in progress, restrict the processing of the Personal Data in question whilst verifying its accuracy, whether or not the individual has exercised their right to restriction;

When accuracy is established, please let the individual requestor know whether or not it will be amended.

In certain circumstances a request for rectification may be refused. This decision should be made with the support of the Data Protection Officer or other suitably qualified persons, having assessed the impact of such refusal.

Erasure

Individuals have the right to have Personal Data erased. As with the other rights already discussed, the right to erasure (aka, to be forgotten) is not absolute and only applies in certain circumstances.

Personal Data may be erased for reasons such as:

- the Personal Data is no longer necessary for which it was originally collected or processed;
- the Controller is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- the Controller is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the Controller is processing the Personal Data for direct marketing purposes and the individual objects to that processing; or
- the Controller must do it to comply with a legal obligation.

The right to erasure may not apply if processing is necessary for, without limitation, the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- processed in accordance with Article 29(1)(h)(ix); or
- for the establishment, exercise or defense of legal claims.

Restriction

Individuals have the right to restrict or limit the processing or use of their Personal Data in certain circumstances. Restricting is a reasonable alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their Personal Data where they have a specific reason for it. Such reasons may include issues with the content of the information held, or how the data is processed. It does not necessarily mean that the limitation will continue indefinitely, but it will need to be in place for a certain period of time.

Restricting processing can be achieved by:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

When a responding entity considers a request for restricting processing or when the decision has been made to restrict processing Personal Data, it must not process the restricted data in any way unless certain specific exceptions apply to be determined on a case by case basis or unless the individual requestor permits it again.

As restricting is often temporary, a responding entity must inform the Individual requestor making the request before removing any restricting or processing the data again.

Objection and Automated Decision-Making

Individuals may object at any time on reasonable grounds relating to his particular situation to the processing of Personal Data relating to him.

Individuals also have the right to be informed before Personal Data is disclosed for the first time to third parties or used for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses.

The right to object only applies in certain circumstances. Whether it applies depends on the purposes for processing and the Controller's stated lawful basis for processing.

Individuals always have the right to object to processing Personal Data for direct marketing purposes. However, the right to object may be limited in other situations, such as where the processing is for:

- a task carried out in the public interest
- the exercise of official authority
- legitimate interests of the Processor or a third party; or
- research or statistical purposes

Such determinations will be made with the review and approval of the Data Protection Officer or other suitably qualified persons, having assessed the impact on the individual's rights of limited this objection.

Where an objection is raised and there are no grounds to refuse the objection, a responding entity must stop processing the data. This may also mean the Personal Data must be erased. However, this will not always be the most appropriate action, for example if the processing is for other purposes as the data must be retained the data for those purposes. For example, when an individual objects to the processing of their data for direct marketing, it may be appropriate to place their details onto a suppression list to ensure continued compliance with the objection.

In addition to the above, and with a few limitations, an individual requestor may object to any decision based solely on automated Processing, including Profiling, which has legal or other seriously impactful consequences. He or she may request that such decision is reviewed manually.

Article 38 addresses automated decision-making and profiling. To clarify, certain limitations on objecting to automated decision-making / profiling, DIFC law and policies and UAE law concerning fraud, counter-terrorism, money laundering, and tax-evasion monitoring / prevention, even where it produces legal consequences concerning a Data Subject, is regarded as falling within Article 38(2)(b).

Notification of Disclosure

Article 36 requires that a responding entity communicates any rectification or erasure of Personal Data or Processing restriction carried out in accordance with Articles 33, 34 and 35 to each recipient to whom the Personal Data has been disclosed, unless doing so proves impossible or involves disproportionate effort. The responding entity will inform the individual requestor about those recipients upon request.

Portability

An individual requestor may ask to receive Personal Data previously provided to the responding entity in a structured, commonly used and machine-readable format where the Processing is based on consent or the performance of a contract executed and carried

out by automated means. The purpose of Article 37(1) is to enable ready portability between Controllers if so requested, in which case Personal Data should be transmitted directly from a Controller to whom the request is made to any other entity, where technically feasible.

5. Non-discrimination

Rights explained

Article 39 introduces the concept of **non-discrimination** where a Data Subject who exercises any rights under DP Law Part 6 is concerned. This important concept protects individuals from retaliation and ensures that even where a SAR or other right is exercised, an entity makes only reasonable, objective changes to offers, pricing, or quality of goods or services. Article 39 also clarifies that Data Subjects have the right to withdraw without penalty from, and require the cessation of processing carried out under, any incentive scheme at any time. These additions to the DP Law are based on assurance of fairness in evaluating and responding to a request to exercise one's rights. As mentioned above, generally, motivation of the individual for making a request is not to be considered by the parties required to respond.

However, due to the often contentious nature of such requests, and in some cases, the costs, a responding party may be tempted to recover fees through pricing changes or to create difficulties receiving services for the requestor. It is recommended again to disregard motive or the perception of impropriety or ill-will when an individual makes a valid request for access to information or to exercise other privacy rights, subject to the rare occasion on which limitations or exemptions (as outlined above) could be exercised.

Should an individual experience perceived discrimination in breach of Article 39, he or she may seek redress in accordance with Part 9 of the DP Law.

6. Withdrawing Consent, Cessation of Processing

Rights explained

Withdrawing consent

Underpinning individual requestor's rights in international data protection law is the concept of consent, and this is no different under the DIFC DP Law. A Data Subject / individual requestor may withdraw consent at any time by notifying a Controller in accordance with Article 32 of the DP Law.

In certain instances, this is an absolute right, but generally, the Controller must comply as soon as reasonably practicable and must ask its Processors to do the same.

Cessation of Processing

While this is not directly a Data Subject's right under Part 6 of the DP Law, Article 22 requires that where, among other issues, a Controller is required to cease Processing due to the exercise of a Data Subject's rights, and must therefore ensure that 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; or
d) securely encrypted.

Personal Data cannot be 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.[5]

In limited circumstances set out in Article 22(4), the above may not be required, but a data protection impact assessment and policy / process for managing such Personal Data when the grounds in Article 22(4) no longer apply must be in place.

[5] *To be sure, pseudonymised data is Personal Data, in accordance with UK ICO guidance.*

7. Administrative Matters

Additional information to support your SAR

Making a Request

Similar to the SAR, an individual requestor can make a request for any of the above actions verbally or in writing, and the response must be provided within one (1) month of the request and free of charge, subject to any other applicable conditions set out in the relevant provisions of the DP Law. The individual requestor should provide as much detailed information as necessary at the outset so that the response can be provided as promptly as possible. In order to assist with responding to such requests, please consider using the rights request response assessment tool available on the Guidance page of the DIFC DP website.

Fees

Subject to the information provided above, while a responding entity should normally take action free of charge, it may charge reasonable fees, based on the magnitude of administrative costs of complying with the request. The individual requestor should, without undue delay, be contacted to explain the decision to charge a fee. Where applicable, compliance with a request is not required until the fee is received.

Complaints

Where a request to exercise individual rights has been refused, an unjustified fee has been charged, or the request has been handled in a manner such that the outcome is not reasonably satisfactory, individuals have the right to make a complaint to the Commissioner of Data Protection or another supervisory authority (where applicable). As a result, any decisions or explanations involved in the request response may be reviewed and/or further action taken, as the Commissioner in his independent judgement deems appropriate. In certain cases where the request is denied, individuals may seek to enforce your rights through a judicial remedy set out in Part 9 of the DP Law.

Please also see the Complaints guidelines available on the Accountability & Rights page of the DIFC DP website, the related guidance on Complaints and Mediation, as well as the Individual Rights & Remedies Table checklist. Additional support, including an assessment tool to help you understand how to respond to any individuals' data rights request, can is available on the Guidance page of the DIFC DP website.

8. Questions and Comments

Please contact the DIFC Commissioner of Data Protection either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office for any clarifications or questions related to this document. You may also wish to refer to the DIFC Online Data Protection Policy.