DIFC DATA PROTECTION POLICY GUIDANCE

Commissioner of Data Protection

INDIVIDUALS' RIGHTS TO ACCESS AND CONTROL DIFC PERSONAL DATA PROCESSING

Contents

1. Introduction and Scope

The Dubai International Financial Centre and/or its affiliates and entities (collectively "DIFC", "DIFCA", "we" or "us") values individuals' security and privacy. DIFC has its own data protection law, Data Protection Law, DIFC Law No. 1 of 2007 (the "DP Law"), and may for certain types of personal data processing also apply the laws from other jurisdictions.

Under DIFCA law and others like it, individuals ("requestor", "individual", "you", or the plural of these terms) about whom we collect and process personal data have fundamental rights to know about such activities. Articles 17 and 18 of the DP Law ensure that any individuals have the right to access, rectification, erasure or blocking of the personal data that DIFCA processes about them, if any. You also have the right to object to such processing. As DIFCA, in addition to being a regulator, is also a data controller (a "controller"), the following information addresses how an individual may exercise these rights.

For more general information about how DIFC manages personal data that it collects, please see the DIFC Online Data Protection Policy.

2. Subject Access Requests

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.

2.1 How to make 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, we may be required to communicate with you 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*: we "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.
- *Refine the scope of the personal data requested:* We may ask questions to get a better understanding of the universe of data requested and will indicate potential technological or other issues in advance to ensure a response that is reasonably appropriate, useful and informational for you. Compliance with the SAR is only required once such information is received.
- *Searching for personal data requested*: We will use appropriate measures to exhaust our search for the personal data you request, but will notify you 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. We will agree the format of the response with you in advance if possible. Also, before supplying any information in response to a SAR, we will check that your postal or email address or any other contact information to which the data is to be sent is correct.

2.2 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, you 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; and
- given details of the source of the data (where this is available and disclosable).

2.3 Potential Exclusions and Exemptions

We reserve the right to exclude data that does not qualify as personal data or may not be appropriately responsive to the SAR. For example, we may exclude anonymous data, or notations that are purely internal to the DIFCA and 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. Even if the third party has not consented, it may still be reasonable to include the data in the SAR response where disclosure is reasonable under the circumstances.

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 will first be approved by both the Director of Data Protection and a senior manager in the BU (where applicable). Where any redaction of information is permitted on whatever basis, the SAR response will clearly and fully explain, to the extent practical, the fact that information has been withheld and the reasons why.

2.4 Response Time

In accordance with the DP Law, the response to the SAR must be provided without excessive delay. In certain circumstances, it may take a considerable amount of time to properly search for the personal data requested. In these cases, we will continue to communicate with you about any timing issues and potential resolutions.

2.5 Fees for SARs

The information should be provided free of charge unless the request results in high administrative costs or you request additional copies of the documentation provided.

3. Rectification, Erasure, Blocking or Objection

Articles 17 and 18 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.

3.1 Rectification

Rectification is the right of individuals to have inaccurate personal data rectified, or completed if it is incomplete. Best practice suggests we:

- Verify the accuracy of data by whatever factual means available, including discussions with and collecting data from you;

- 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, we will let you know whether or not it will be amended.

In certain circumstances a request for rectification may be refused, but only upon review and approval by the Director of Data Protection and / or the Commissioner of Data Protection.

3.2 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, in the discretion of the Commissioner, 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; or
- for the establishment, exercise or defense of legal claims.

3.3 Blocking

Individuals have the right to block or limit the processing or use of their personal data in certain circumstances. Blocking is a reasonable alternative to requesting the erasure of their data.

Individuals have the right to block 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.

Blocking 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 we are considering a request for blocking or when the decision has been made to block processing personal data, we will not process the blocked data in any way unless certain specific exceptions apply to be determined on a case by case basis or unless you ask us to.

As blocking is often temporary, we will inform you before removing any blocking or processing the data again.

3.4 Objection

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

You 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 data 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 Director of Data Protection and/or the Commissioner of Data Protection.

Where an objection is raised and there are no grounds to refuse the objection, we will 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.

4. Making a Request

Similar to the SAR, you can make a request for any of the above actions verbally or in writing, and the response must be provided without excessive delay or expense. Provide as much detailed information as necessary at the outset so that we may respond as promptly as possible.

5. Fees

While we will normally respond to these requests free of charge, we may charge reasonable fees, based on the magnitude of administrative costs of complying with the request. We will without undue delay contact you to explain the decision to charge a fee. Where applicable, compliance with your request is not required until the fee is received.

6. Complaints

Where a request to exercise individual rights has been refused or handled in a manner such that the outcome is not satisfactory to you 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, you may seek to enforce your rights through a judicial remedy.