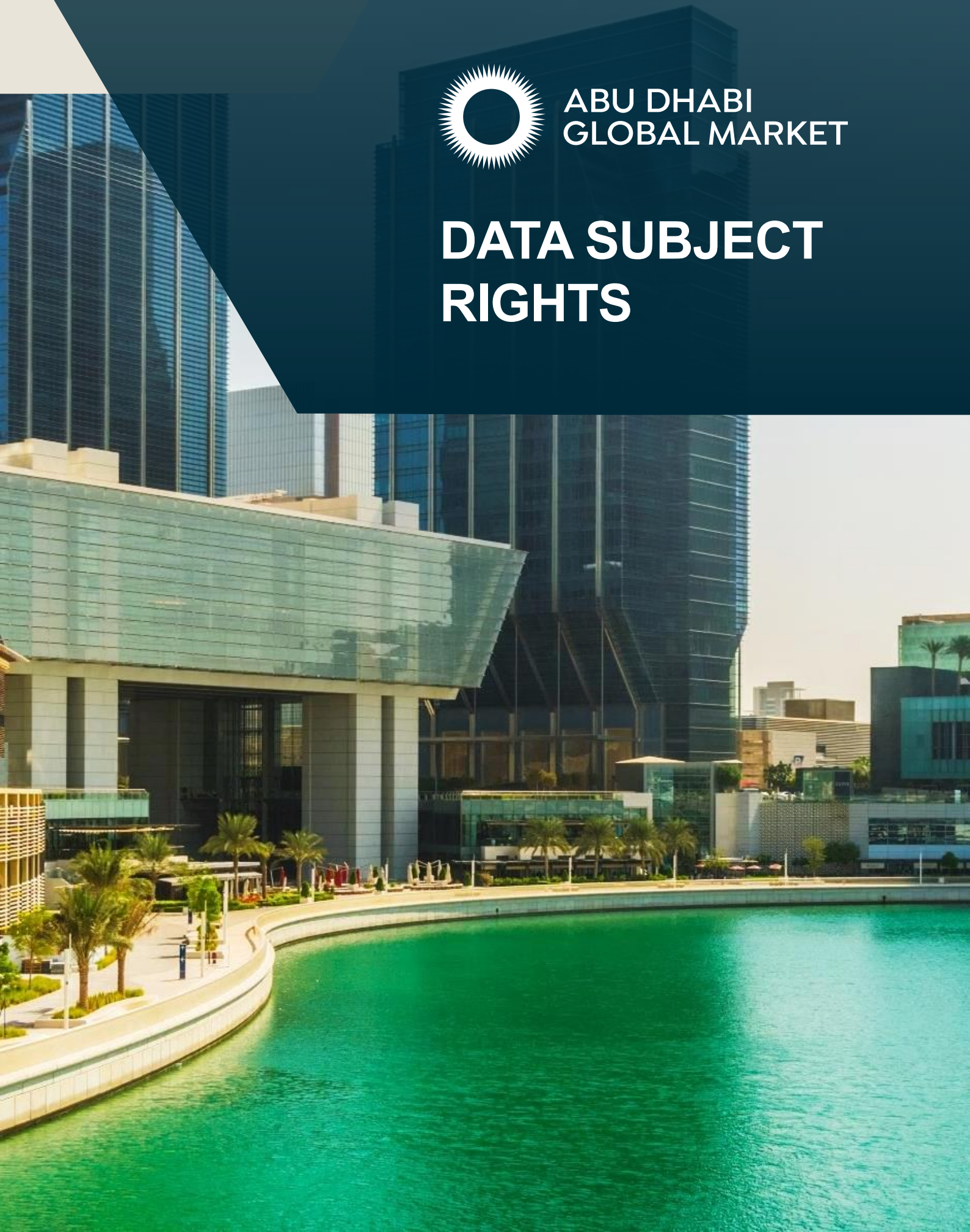
ABU DHABI GLOBAL MARKET

DATA SUBJECT RIGHTS



Introduction

Individuals whose personal data is collected, stored, processed, or shared are called ‘Data Subjects’. Under the ADGM Data Protection Regulations 2021, Data Subjects are provided certain rights which they may exercise against Controllers or Processors.

An individual may file a complaint with the Commissioner of Data Protection if they feel that their personal data has been improperly handled or if any of the rights in the Regulations have been violated.

What type of rights do Data Subjects have?

Data Subjects have numerous rights under the Regulations. This includes the right to be informed, to access their personal data, request erasure, right to data portability, restriction, or rectification of their personal data or to object to its use. These and other rights are described within this brochure. It is important to note that these rights are not absolute. Rights can be restricted in specific cases.

What obligations do Controllers have in relation to Data Subject’s rights?

The Controller must take appropriate measures to provide individuals with relevant and adequate information while also keeping them informed of their rights:

Controllers must make sure that the communications with Data Subjects in relation to requests to exercise their rights are clear and easy to understand. This is even more important if the Data Subject is a child.

Controllers must “facilitate” the exercise of Data Subject Rights. This means that a Controller must help Data Subjects understand and exercise their rights. This could include explaining how a particular right applies, or helping an individual to narrow down a very large request which the Controller might otherwise consider unreasonable or excessive.

Controllers must not refuse to act on a request to exercise rights unless they can show that:

- they are unable to identity the Data Subject
- the request is unreasonable or excessive

What are the Data Subject rights in the DPR 2021?

Right to be informed

The right to be informed means that Controller must tell Data Subject about the processing of their personal data. Controllers usually do this by providing a privacy notice or privacy policy which contains the required information. Information should be provided in such a way that it is concise, transparent, intelligible, easily accessible, and uses clear and plain language.

Controllers should avoid any language which is legalistic or uses industry specific terminology (unless that terminology is explained in such a way that an ordinary person would understand it).

Right of access

The right of access gives Data Subjects the right to request from the Controller

- confirmation of whether or not the Controller is processing the individual's personal data; and
- a copy of such data

In addition, the Controller must give the Data Subject certain information about the processing which is set out in Regulations. This information must be provided without undue delay and in any event within two months of receipt of the request. This may be extended by one month in certain circumstances.

Right to rectification

Data Subjects have the right to have any:

- inaccurate personal data corrected; and
- incomplete personal data completed

Controllers should take reasonable steps to ensure that the data is accurate and correct the data if necessary.

Right to data portability

The right to data portability is intended to allow Data Subjects to obtain and re-use their data for their own purposes and across different services.

- Where technically feasible, individual can request a copy of their personal data or have the Controller transmit the data to another Controller
- In both cases the data must be provided in a structured, commonly used and machine-readable format.

Right to object

If the right to object applies, an individual can object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent Controllers from processing their personal data, such as when processing is for direct marketing, automated processing, or profiling. Controllers should not process personal data subsequent to an objection unless:

- a legitimate reason for the processing overrides the rights of the Data Subject;
- processing is necessary in order to establish, exercise, or defend legal claims.

Right to erasure

The Data Subject has the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller has the obligation to erase personal data without undue delay where one of the following applies:

- the personal data is no longer necessary for the purpose for which it was collected or processed
- the processing was based on consent, the Data Subject withdraws consent and there is no other legal basis for the processing
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing to continue
- the Data Subject objects to the processing of their data for direct marketing purposes
- the personal data has been unlawfully processed
- the personal data has to be erased for compliance with a legal obligation in Applicable Law (as defined in the DPR 2021) to which the Controller is subject

Right in relation to automated decision making and profiling

An individual has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant effects concerning him/her. This right does not apply when:

- the decision is necessary for entering into or performing a contract with the Data Subject
- Controller has the Data Subject's explicit consent
- the decision is required or authorized by Applicable Law

The individual does not need to actively exercise this right. It is essentially an obligation placed on data Controllers not to make such decisions in the manner described.

Right to restriction

Individuals can require Controllers to restrict the processing of their personal data in certain circumstances. The right is available where:

- an individual contests the accuracy of their data, while the Controller is verifying the accuracy of the data
- the processing is unlawful and the Data Subject requests restriction instead of erasure
- the Controller no longer needs the personal data for the purposes of processing but is required by the Data Subject for the establishment, exercise, or defense of legal claims
- the Data Subject has exercised their right to object to processing based on the "legitimate interest" basis while the Controller verifies whether its legitimate grounds override those of the Data Subject

Restriction of processing means that a Controller cannot use the data for anything apart from:

- with the Data Subject's consent
- for the establishment, exercise or defense of legal claims
- for the protection of the rights of another natural or legal person
- for reasons of important public interest

The Controller is however, able to store the data.

What information needs to be provided to individuals when personal data is collected?

Controllers are required to provide certain information when they obtain personal data. The information which must be given to individuals is slightly different depending on whether you obtained the personal data from the Data Subjects themselves or from a third party. The information you must provide is summarized in the table below.

Information	Personal data obtained from Data subject	Personal data obtained from someone other than Data Subject
Identity and the contact details of the Controller	☑	☑
Contact details of the Data Protection Officer	☑	☑
Purposes of processing	☑	☑
Legal bases for the processing	☑	☑
Where the processing is based on the “legitimate interests” legal basis, a description of the legitimate interests relied upon.	☑	☑
The categories of personal data processed	☐	☑
Recipients or categories of recipients of the personal data	☑	☑
Details of any international transfers of the personal data, i.e. transfers to a recipient outside the ADGM or to an international organization	☑	☑
Where an international transfer is made, details of the appropriate or suitable safeguards relied upon and details of how the individual can view/obtain a copy	☑	☑
The period for which the data will be stored, or the criteria used to decide such period	☑	☑
Details of the Data Subject’s rights	☑	☑
If the lawful basis is consent, that consent can be withdrawn at any time and that withdrawal will not affect the lawfulness of processing prior to such withdrawal	☑	☑
The right to lodge a complaint with the Commissioner of Data Protection	☑	☑
Whether providing personal data is a requirement under Applicable Law, a contractual requirement, or a requirement necessary to enter into a contract	☑	☑
Whether the Data Subject is obliged to provide the data, and possible consequences of not providing it	☑	☐

Information (continued)	Personal data obtained from Data subject	Personal data obtained from someone other than Data Subject
The source of the personal data, including whether it came from publicly available sources	☐	☑
Whether automated decision-making, including profiling, is taking place, and meaningful information about the logic involved, as well as the significance and consequences for the Data Subject.	☑	☑
If the data will be processed in a way which restricts the rights to rectification, erasure or objection, an explanation of the impact on such rights	☑	☑
If the data is further processed for a different purpose than that for which it was originally collected, information about this further processing, before it starts	☑	☐

What are the time limits for responding to requests?

Controllers must respond to requests without undue delay and within a maximum of two months from receipt of the request.

The two month period can be extended by a further month (giving a total period of three months) where Controllers need extra time due to:

- the complexity of a particular request; and/or
- the number of requests received

When assessing the complexity and number of requests Controllers can take into account requests which appear to be related to the one they are dealing with, even if they have come from different Data Subjects.

- If the Controller decides to extend the time period for response to three months, they must tell the Data Subject this within the first two months, and also explain the reasons for the delay.
- If the Controller needs to ask the Data Subject for additional information to confirm their identity the time period (two or three months) does not start until Controller has received this information.

Can a Controller refuse to comply with the request?

The Regulations state that a Controller can refuse to comply with a request which is unreasonable or excessive, in particular because it is repetitive. If Controller refuse a request on this basis they are responsible for demonstrating that the request is in fact unreasonable or excessive.

The Regulations do not define what is meant by unreasonable or excessive, however, this will be a high threshold to meet. If Controller refuse to action a request on this basis they must notify the individual and explain the reason for exemption.

Can the Controller charge a fee?

No, generally speaking Controllers must deal with requests free of charge. The only exception to this is where a request is unreasonable or excessive, in particular because it is repetitive. In this case a Controller can either refuse to deal with the request or charge a reasonable fee to cover the administrative costs.

Should the Controller ask for proof of identity?

If a Controller has reasonable doubts over the identity of the person making the request, the Controller can ask the individual for more information to confirm their identity. However, the Controller cannot rely upon requests for information as a method to delay and frustrate requests from Data Subjects when they can otherwise identify the individual from information currently in their possession. The time period for responding to the request does not start until a Controller has received the additional information needed to confirm identity. If a Controller is asking for additional information they should do this promptly. It would not be reasonable, for example, to request additional information six weeks after receiving a request.

In some cases a person or organization may submit a request on behalf of the Data Subject.