ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 2: Data Subjects' Rights

Office of Data Protection

TABLE OF CONTENTS

1. INTRODUCTION

Introduction to this Guidance

1.1 This is Part 2 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). It covers the rights which data subjects have under the DPR 2021:

- The right to be ***informed*** about processing;
- The right to ***access*** personal data;
- The right to ***rectification***;
- The right to ***erasure/deletion***;
- The right to ***restriction***;
- The right to ***data portability***;
- The right to ***object***; and
- Rights in relation to ***automated decision making*** and ***profiling***.

2. CONTROLLER'S OBLIGATIONS

2.1 What are the controller's obligations in relation to data subjects' rights?

- You must make sure that your 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.
- You must "facilitate" the exercise of data subject rights. This means that you 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 you might otherwise consider unreasonable or excessive.
- You must not refuse to act on a request to exercise rights unless you can show that you are unable to identify the data subject (or the request is unreasonable or excessive – see paragraph 2.5 below).

2.2 What are the time limits for responding to requests?

You 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 you 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 you can take into account requests which appear to be related to the one you are dealing with, even if they have come from different data subjects.

If you decide to extend the time period for response to three months, you must tell the data subject this within the first two months, and also explain the reasons for the delay.

If you need to ask the data subject for additional information to confirm their identity (see paragraph 2.4 below) the time period (two or three months) does not start until you have received this information.

Example:

An organisation is in a dispute with a group of individuals who have launched a claim against it. The organisation receives a large number of subject access requests from members of the group bringing the claim.

The organisation considers these requests to be related even though they have been submitted by different individuals. It considers that due to the large number of requests received from this group, it is unable to respond in the normal two month timeframe and replies to all the data subjects to inform them that it is extending the timeframe for response to three months because it has received a high number of requests which appear to be related.

Example:

A business receives a subject access request from an employee who has been employed by the organisation for 20 years. The employee requests a copy of all personal data the employer holds about him. The business considers this a complex request due to the amount of personal data it holds about the individual and the number of different systems and records it will have to search. It therefore explains this to the employee and lets him know he will receive a response within three months.

2.3 What if a data subject makes multiple requests?

Each request from a data subject should be dealt with individually. For example, where a data subject validly makes both an access request and a data portability request, the controller should provide the data subject with his or her personal data, as well as providing it to the other controller (as instructed by the data subject) in the format required under section 18 (1) of the DPR 2021.

2.4 Should we ask for proof of identity?

If you have reasonable doubts over the identity of the person making the request, you can ask the individual for more information to enable you to confirm their identity. However, you cannot rely upon requests for information as a method to delay and frustrate requests from data subjects when you can otherwise identify the individual from information currently in your possession. The time period for responding to the request does not start until you have received the additional information needed to confirm identity. If you are going to ask for

additional information you 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 organisation may submit a request on behalf of the data subject.

Example:

A bank receives an email with a request for access to personal data from an individual who says they are an account holder. The bank requires proof of identity before disclosing any data.

Example:

An employer receives a request for access to personal data from an employee. The request is received through an internal system set up for this purpose. The employer does not request proof of identity in this case as it has no doubts over the identity of the individual.

For example a request could be submitted by a friend or relative of the data subject, or by a solicitor acting for the data subject. This is acceptable provided that you are satisfied that the person submitting the request has the authority of the data subject to do so.

2.5 Can we charge a fee?

No, generally speaking you 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 you can either refuse to deal with the request or charge a reasonable fee to cover your administrative costs.

Example:

A data subject makes a request for copies of all their personal data. The controller carries out a reasonable search and provides the data subject with all personal data which it is able to identify.

Two weeks later the data subject makes exactly the same request. In the context of the controller's processing, the personal data held has not changed in this two week period.

Because of the repetitive nature of this request the controller can either refuse to comply with it (see paragraph 2.6 below) or charge the data subject a reasonable fee to cover its costs in complying with the second request.

2.6 Can we refuse to comply with a request?

Section 10(6) of the DPR 2021 states that you can refuse to comply with a request which is unreasonable or excessive, in particular because it is repetitive. If you refuse a request on this basis you are responsible for demonstrating that the request is in fact unreasonable or excessive.

The DPR 2021 do not define what is meant by unreasonable or excessive, however, this will be a high threshold to meet. If you refuse to action a request on this basis you must notify the

individual and explain why you think the exemption applies (i.e. why you have decided the request is unreasonable or excessive).

An **unreasonable request** may be:

- a request where the individual clearly has no intention to exercise the particular right, for example, an individual makes a request, and at the same time, offers to withdraw it in exchange for something (e.g. a payment); or
- a request which is being used to harass or cause disruption e.g. where:
    - a requester explicitly states that they are making the request for the purposes of causing disruption;
    - a person sends constant requests on a regular basis with the intention of causing disruption; or
    - the individual targets a particular employee or makes unjustified accusations in their request.

Example:

A customer makes a request for erasure to an ADGM entity and also says that he will withdraw the request in exchange for a payment. The entity considers the request to be unreasonable as the individual has no real intention of exercising the right. It decides not to comply with the request and informs the individual accordingly.

Example:

A former employee sends repeated requests to an organisation, addressed to her former manager. The requests contain abusive language and threats against the manager. The organisation considers the requests to be unreasonable and informs the individual that it does not intend to comply on this basis.

When judging whether a request is **excessive** you should consider all the circumstances relating to the request:

- the nature of the request;
- the context in which the request is made, including the relationship between your organisation and the requester;
- how a refusal to action the request will impact the individual; and
- whether the request overlaps with, or repeats, other requests made by the individual.

When considering whether a request is **repeated**, you should take account of the interval which has elapsed between requests, and how often you alter the data you hold about the individual.

See also paragraph 11 for details of restrictions applicable to data subject rights.

3. THE RIGHT TO BE INFORMED

3.1 What is the right to be informed?

The right to be informed means that you must tell people 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).

Information should also be presented in such a way that it is targeted to the intended audience. For example, the tone and content a privacy notice intended for children or adults with a vulnerability which makes it difficult for them to comprehend written information would be different to one addressed to adults without any such vulnerabilities.

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 summarised in the table below.

Information to be provided	Personal data obtained from data subject	Personal data obtained from someone other than data subject
Identity and contact details of the controller	✓	✓
Contact details of the DPO	✓	✓
Purposes of the 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.	✓	✓

Information to be provided	Personal data obtained from data subject	Personal data obtained from someone other than data subject
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 organisation.	✓	✓
Where an international transfer is made, whether or not the recipient country has an adequacy decision from the Commissioner of Data Protection.	✓	✓
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.	✓	

Information to be provided	Personal data obtained from data subject	Personal data obtained from someone other than data subject
Whether the data subject is obliged to provide the data, and possible consequences of not providing it.	✓	
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.	✓	✓

3.2 When must the information be given?

If you obtain the personal data from the data subject, you must give the information about the processing at the same time as you obtain the personal data.

If you obtain the personal data from someone other than the data subject you must provide the necessary information:

- within a reasonable period, but at the latest within two months;
- if the data is to be used to communicate with the data subject, at the time of such communication at the latest; or
- if you disclose the data to a third party recipient, at the time of the disclosure at the latest.

3.3 Are there any exceptions?

If you know, or it's obvious, that an individual already has some of the information about the processing that you are required to provide, you do not need to give that information it to the individual. However, you must still provide them with anything that they don't already have.

Where the personal data is obtained from someone other than the data subject, you also do not have to provide information about the processing if:

- provision of the information is impossible or would involve disproportionate effort;
    - The DPR 2021 do not define what amounts to disproportionate effort but this will be a high threshold which is not easily met.
    - To rely on this exception, you should assess whether there is a proportionate balance between the effort involved for you to provide individuals with privacy information and the impact that your use of their personal data will have on them. The more significant the effect, the less likely you will be able to rely on this exception.

Example:

An ADGM based employer collects details of emergency contacts from its employees. The ADGM based employer determines that the effort involved for it to write to every emergency contact to provide them with privacy information is disproportionate in relation to the effect that the use of their personal data will have on them.

The ADGM based employer decides not to proactively provide privacy information to the emergency contacts but provides information on its website, instructs its employees to make sure that the emergency contacts know that their contact details are being provided to it, and ensures that use of this information is limited by internal controls and policies.

- obtaining or disclosing the data is expressly required by applicable law which provides appropriate measures to protect the data subject's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy, or duty of confidentiality, regulated by applicable law.

Example:

A law firm receives information from their client whom they are defending against a charge. The client provides information to the solicitor about another person who is a co-defendant.

The law firm does not have to tell the other person that it is processing this person's personal data as it received it under a duty of confidentiality owed to its own client.

See also paragraph 11 for details of restrictions applicable to data subject rights.

4. THE RIGHT OF ACCESS

4.1 What is the 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 sections 13(1)(a) to (h) and 13(2) of the DPR 2021. This information largely corresponds to the information which controllers must provide under the right to be informed. It is often contained in an organisation's privacy notice.

4.2 How should we provide data?

If the individual makes the request in electronic form, e.g. by email or by submitting an online form, you should respond in the same way, and provide the data in a commonly used electronic form, unless the individual requests otherwise. Subject access requests need to be assessed on a case-by-case basis. It may not always be appropriate to provide the entirety of a document in which personal data is contained.

Example:

An employee makes a request for his personal data processed by the employer in relation to a disciplinary procedure. One of the documents found by the employer when carrying out a search for the personal data is a set of minutes from an internal meeting discussing the disciplinary process at which the employee was not present.

The employer does not have to provide the full set of meeting minutes in response to the access request as not everything contained in the minutes is the individual's personal data. Instead the employer extracts the personal data and provides this separately.

4.3 Can we charge for copies?

You must provide a copy of personal data free of charge. If the individual requests further copies you may charge a reasonable fee for this, based on your administrative costs. When assessing what is a reasonable fee you can take into account your staff's time in providing additional copies and any materials used if the data is provided in hard copy.

4.4 What if we process a lot of personal data about an individual?

If you process a lot of information about the person making the request, you can ask them to specify the particular information they would like to receive, to the particular processing activities their request relates to. However, you cannot require a data subject to limit their request in this way. If a person wants to receive a copy of all personal data you process, you must provide this.

4.5 Are there any exemptions?

The right to obtain a copy of personal data must not adversely affect the rights of others. The "rights" of others in this context is not limited only to the rights of others under the DPR 2021.

For example, when handling a request to obtain a copy of any personal data, controllers may consider intellectual property rights held by others, or information which constitutes a trade secret. Controllers cannot however rely upon the rights of others to deliberately frustrate an otherwise legitimate request.

Example:

An employee makes a data subject rights request to his or her employer. The employer cannot argue that it is not permitted to disclose the individual's HR file on the basis that the intellectual property rights in the file are actually owned by the employer's parent company, even if that is strictly the case, perhaps because the HR function is run centrally.

Sometimes requests for access involve personal data relating to both the data subject and to other individuals.

Example:

A customer uses an organisation's online chat function to speak to the organisation's customer service team. The customer requests a copy of the transcript. This contains both the requester's personal data and personal data of the customer service employee.

The DPR 2021 say that if the request involves information about other individuals you do not have to comply with the request to the extent that doing so would disclose personal data relating to another person unless:

- the other individual has consented to the disclosure: or
- it is reasonable to comply with the request without the other individual's consent.

If neither of the above apply, you should comply with the request as far as possible without disclosing the other individual's personal data. This is likely to require you to redact the other individual's information. If this is not possible, then you do not have to comply with the request.

Example:

An organisation carries out a recruitment process and holds an internal meeting to discuss the candidates. One of the unsuccessful candidates later makes a subject access request for all personal data relating to the recruitment process.

The minutes of the internal meeting contain personal data relating to both the requester and the other candidates. The business does not have, and cannot easily obtain, the consent of the other candidates to the disclosure. Nor does the business consider it reasonable to provide this information without the other candidates' consent.

See also paragraph 11 for details of other restrictions applicable to data subject rights.

5. THE RIGHT TO RECTIFICATION

5.1 What is the right to rectification?

Individuals have the right to have any:

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

If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and correct the data if necessary. You should take into account the arguments and supporting evidence provided by the data subject.

What steps are reasonable will depend on the nature of the personal data and what you are using it for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it.

Example:

A health insurance provider calculates premiums taking into account customers' health conditions and medical history.

A customer asks the insurer to rectify his personal data as he says that the insurer has a number of health conditions listed on his customer record that are incorrect.

Because the personal data in this case will be used in a way which has a significant effect on the data subject, the insurer will be expected to make a considerable effort to verify accuracy.

If you are satisfied that the data is accurate you should explain this to the individual. It is also good practice to make a note in your systems that the individual has challenged the accuracy of the data and their reasons for contesting the accuracy.

5.2 Are there any exceptions?

There is a limited exception to the right to rectification which applies where:

- it is not feasible to rectify data for technical reasons;

Example:

A Fintech platform which stores personal data on a blockchain receives a request from a user to rectify his or her personal data. The platform operator may rely upon this exemption if it is not possible to rectify the data which has been already uploaded to the blockchain for technical reasons (provided the other requirements below have also been met).

- you obtained the personal data from the data subject; and
- you told the data subject (e.g. in the data protection notice given to them) that rectification of personal data at his/her request would not be feasible.

See also paragraph 11 for details of restrictions applicable to data subject rights.

5.3 Do we need to tell other organisations if we rectify personal data?

If you rectify personal data you need to tell other organisations and individuals with whom you have shared the data about the rectification unless this is impossible or requires disproportionate effort. When deciding if the effort required is disproportionate you should take into account the number of data subjects, the age of the data, and the appropriate safeguards adopted.

6. THE RIGHT TO ERASURE

6.1 What is the right to erasure?

In certain circumstances the data subject can require the controller to erase his/her personal data. This right is available where one of the following applies (although see also paragraph 6.2 for situations where the controller can refuse to erase data):

- 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; or
- 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.

Example:

A business receives a request for erasure from a former customer. The business has no current relationship with the individual and uses the individual's personal data for direct marketing purposes only. It therefore erases the data following the individual's request.

6.2 When can we refuse to comply with a request for erasure?

You do not need to comply with a request for erasure in certain limited circumstances. You should review section 15(3) of the DPR 2021 for the full list of circumstances and conditions which apply. They may be relevant to you if the processing you are carrying out is necessary for:

- compliance with a legal obligation;
- reasons of public interest in the area of public health;

- archiving and research purposes; or
- the establishment, exercise or defence of legal claims.

Example:

A customer buys some make up products from an online cosmetics company. The customer sends a written complaint about the products, and then later requests for all their personal data to be deleted.

The business assesses the request and decides that it needs to retain certain of the customer's personal data on the basis that it is necessary for the defence of legal claims given the complaint received from the customer.

There is an additional limited exception to the right to erasure which applies where:

- erasure is not feasible to erasure data for technical reasons;
- you obtained the personal data from the data subject; and
- you told the data subject (e.g. in the data protection notice given to them) that erasure of personal data at his/her request would not be feasible.

See paragraph 5.2 above for an example of this exception. See also paragraph 11 for details of restrictions applicable to data subject rights.

6.3 Do we need to tell others about the request or erasure?

If you have made personal data public and receive a request for erasure of that data that you must comply with, you should take reasonable steps to inform other controllers that a request for erasure has been made.

The DPR 2021 do not define what is meant by reasonable but you should take into account the available technology and cost of implementation.

If you erase personal data you also need to tell other organisations and individuals with whom you have shared the data about the erasure unless this is impossible or requires disproportionate effort. When deciding if the effort required is disproportionate you should take into account the number of data subjects, the age of the data, and the appropriate safeguards adopted.

7. THE RIGHT TO RESTRICTION

7.1 What is the right to restriction?

Individuals can require you 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 it is required by the data subject for the establishment, exercise or defence of legal claims; or
- 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.

Example:

An individual contests the accuracy of their personal data held by a credit reference agency. Whilst the agency verifies the accuracy of the data it restricts the processing, meaning that it does not use the data to generate any credit scores or reports in respect of the individual.

7.2 How do we restrict processing?

Restricting processing means that you cannot use the data for anything apart from:

- with the data subject's consent;
- for the establishment, exercise or defence of legal claims;
- for the protection of the rights of another natural or legal person; or
- for reasons of important public interest.

You are however, able to store the data.

You are likely to need to put processes in place to enable you to restrict processing if required. Although there are no specific measures or actions required by the DPR 2021, you might want to consider the following, if relevant to your organisation:

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

You must tell the data subject before you lift the restriction.

7.3 Do we need to tell other organisations if we restrict processing?

If you restrict the processing of personal data you need to tell other organisations and individuals with whom you have shared the data about the restriction unless this is impossible or requires disproportionate effort. When deciding if the effort required is disproportionate you should take into account the number of data subjects, the age of the data, and the appropriate safeguards adopted.

8. THE RIGHT TO DATA PORTABILITY

8.1 What is the right to data portability?

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

If the right applies (see paragraph 8.2 below) an individual can request a copy of their personal data or have the controller transmit the data to another controller, where technically feasible. In both cases the data must be provided in a structured, commonly used and machine-readable format. You should consider the technical feasibility of a transmission to another controller on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations.

Example:

A bank receives a request from a customer to transfer his or her bank statements to a potential third party lender, who the customer is seeking a loan from. The third party lender uses a specific platform to receive and send bank customer documents, such as bank statements. If the bank does not use that same platform then it does not have to subscribe to the same platform, or develop a piece of software which is compatible with it.

It would be sufficient for the bank to provide the statements in, for example, CSV, XML and JSON formats, or to allow the customer to download those from his or her online banking account in such formats.

As an alternative to providing the data you could also provide access to an automated tool that allows the individual to extract the requested data themselves.

8.2 When does the right apply?

The right to data portability only applies:

- to personal data which a data subject has provided to a controller (and not to data which a controller has received from someone other than the data subject);
- where processing is based on the legal basis of consent (section 5(1)(a) or 7(2)(a) of the DPR 2021), or where processing is necessary for a contract (section 5(1)(b) of the DPR 2021); and
- where processing is carried out by automated means.

The right applies to data held by a controller and also to data held on behalf of a controller (e.g. by a processor acting on behalf of the controller).

Example:

A supermarket which offers home delivery keeps records of customers' orders. Customers can view these in their online accounts which they access via the supermarket's website, and there is an automated tool which enables the customers to download their orders themselves.

Example:

An employer in the ADGM uses a third party payroll provider to process employee salary payments. Under section 18(1) of the DPR 2021, the employee may ask the third party payroll provider (as processor of its personal data) to provide a copy of any personal data which it holds on the employee (e.g. Information regarding salary payments, in the form of payslips) in a structured, commonly used and machine-readable format.

8.3 What is a structured, commonly used and machine-readable format?

These terms are not defined in the DPR 2021 but can be broadly understood as follows:

- **Structured**
  - Structured data refers to data where the structural relation between elements is explicit in the way the data is stored on a computer disk.
  - Software must be able to extract specific elements of the data.
  - If a format is structured, it is also often machine-readable.
- **Commonly used**
  - The format must be widely used and well-established.
- **Machine-readable**
  - In a format that can be automatically read and processed by a computer.

Where no specific format is in common use within your industry or sector, you should consider providing personal data using open formats such as CSV, XML and JSON.

9. THE RIGHT TO OBJECT

9.1 What is the right to object?

If the right to object applies (see paragraph 9.2 below) an individual can object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data.

9.2 When does the right to object apply?

The right to object applies where personal data is being processed,

- on the "***public task***" legal basis (section 5(1)(e) of the DPR 2021) . If you receive an objection and you are processing personal data on this legal basis, you must stop processing unless:

    - **you have legitimate grounds for the processing which override the interests and rights of the data subject**. In the course of deciding whether you have legitimate grounds for the processing which override the interests and rights of the individual, you must take into account the reasons on which they are objecting to your processing of their personal data. If the processing is causing the individual substantial damage or distress, this will carry greater weight than processing which causes them some minor inconvenience. Remember that you bear the responsibility for being able to demonstrate that your legitimate grounds override the interests and rights of the individual; or

    - **the processing is necessary for the establishment, exercise or defence of legal claims**. This prevents a data subject from frustrating a legal claim through the exercise of the right to object.

    Example:

    The Financial Services Regulatory Authority may process the personal data of directors of regulated entities in order to perform its regulatory functions, which may involve bringing legal actions against those directors. The directors could not exercise the right to object to prevent the FSRA from processing their personal data for the purposes of those legal actions.

- on the "***legitimate interests***" legal basis (section 5(1)(f) of the DPR 2021). If you receive an objection and you are processing personal data on this legal basis, you must stop processing unless:

    - you have legitimate grounds for the processing which override the interests and rights of the data subject; or

    - the processing is necessary for the establishment, exercise or defence of legal claims. This prevents a data subject from frustrating a legal claim through the exercise of the right to object.

Example:

A company in the ADGM processes an employee's personal data on the basis of legitimate interests and makes that clear in its employee privacy notice. Provided that the personal data is necessary for the purposes for which it was collected (e.g. employee administration, payroll, performance review, etc.), the employer may continue to process the employee's data following the employee' exercise of the right to object on the basis that it continues to have legitimate grounds which override the interests and rights of the data subjects. Employers need to have certain data on their employees in order for the employee-employer relationship to function effectively and this would likely be "legitimate grounds".

Example:

A bank shares information about suspected fraudulent transactions with other financial institutions on the "legitimate interest" legal basis (section 5(1)(f) of the DPR 2021). A customer of the bank objects to all processing of his personal data carried out on this basis because the individual is in an ongoing dispute with the bank. The bank assesses its legitimate grounds for this processing against the interests and rights of the customer and concludes that its legitimate grounds override the interests and rights of the customer. It therefore continues this processing activity and informs the individual accordingly.

- for the purposes of ***direct marketing***, including profiling. If you receive an objection to processing for direct marketing purposes, you must stop using the data for this purpose. It is an absolute right and there are no exceptions to it.

Example:

A bank sends regular emails to its customers to inform them of new products and services which it considers may be of interest to those customers. If the customer contacts the bank making it clear that it no longer wishes to receive those communications, the bank must respect this and stop sending direct marketing materials to the customer. The customer would not need to expressly state that they are "exercising the right to object" and it would not matter that the customer had previously failed to exercise this right (e.g When asked at the time their email address was collected for direct marketing purposes).

It is not always necessary to seek consent under the DPR to conduct direct marketing activities, such as sending marking emails. In many cases, it will be possible to rely upon legitimate interests (see section 5(1)(f) of the DPR 2021) as the relevant legal processing. If you are doing this, it is important to ensure that individuals are given the right to object both at the point at which their personal data is collected for direct marketing purposes, and within each communication (for example, by way of an "unsubscribe link" in an email). A pre-ticked box may be sufficient when offering the right to object at the point of data collection.

Whenever you are relying on legitimate interests as the legal basis for processing for direct marketing, consider whether the legitimate interests in conducting the marketing are overridden by the interests or rights of the data subject. Depending on the context of the direct marketing activities (for example, if the content of those marketing communications relates to products or services which are sensitive in some way, such as health related services), there may be instances where it will not be appropriate to rely on this as the relevant legal basis and consent would be more appropriate.

Controllers must also ensure that they continue to meet their obligation to comply with the principles of transparency and fairness under section 4 of the DPR 2021 by clearly describing their direct marketing activities in the applicable privacy notice.

- for ***Archiving and Research Purposes***. If you receive an objection you must stop the processing unless it is necessary for the performance of a task carried out for reasons of public interest.

The phrase "Archiving and Research Purposes" means:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes in accordance with section 9 of the DPR 2021.

9.3 Objections to processing based on the public task or legitimate interests legal bases

Individuals who object on either of these bases must make their objection on grounds relating to their particular situation. This means that they must give specific reasons why they are objecting to the processing which are based on their own individual circumstances.

If you determine that you do not need to comply with the request either because you have legitimate grounds for the processing which override the interests and rights of the individual, or because you need to process the data for the establishment, exercise or defence of legal claims, you must inform the individual with an explanation of your decision.

9.4 What do we need to tell people about the right to object?

The DPR 2021 say that you must inform individuals about their right to object no later than at the time of the first communication you have with that individual. This will be relevant to you, and you need to inform individuals of this right, if:

- you process personal data for direct marketing purposes; or
- your lawful basis for any processing activity is:
    - the "***public task***" legal basis (section 5(1)(e) of the DPR 2021); or
    - the "***legitimate interests***" legal basis (section 5(1)(f) of the DPR 2021); or
- you process personal data for Archiving and Research Purposes.

When you bring the right to object to the attention of individuals, you must present it clearly and separately from any other information.

10. RIGHTS RELATING TO AUTOMATED INDIVIDUAL DECISION MAKING INCLUDING PROFILING

10.1 What rights do individuals have?

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 (unless one of the criteria explained in paragraph 10.2 applies). 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.

Automated processing is processing which is carried out solely by automated means with no human involvement.

Example:

An ADGM based lender has developed a tool which analyses an individual's financial position in order to determine whether or not they are a suitable candidate for a loan. If the tool determines that they are not a suitable candidate for a loan, then there would be a significant affect on the individual (i.e. they would not have access to credit they were seeking).

Profiling is any form of automated processing consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict

aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Example:

An ADGM based share trading platform tracks the behaviour of its users on the platform through cookies and uses an algorithm (which also draws personal data from the user's account, as provided by the user) to then determine the limit at which the user is permitted to make trades (i.e. a financial cap). This produces a similarly significant effect on the user as he or she may be limited in his or her ability to purchase shares.

Example:

An employer uses aptitude tests as part of its selection process. The tests are automated and, using candidates' responses to a number of questions, generate reports indicating the personality attributes of the candidates.

Example:

A website operator uses cookies to track the browsing habits of customers using its website. It uses the results of this tracking to build up profiles of its customers, such as likely age, location, spending habits and interests. These profiles are used by the website operator to personalise marketing towards its customers.

Legal effects/similarly significant effects are not defined in the DPR 2021, although these terms can be understood as follows:

- A decision producing a **legal effect** is one which affects a person's legal status or rights (e.g. an individual's right to work in ADGM).

- A decision producing **similarly significant effect** is one which has a similar impact on an individual as one which affects an individual's legal status or rights (e.g. an individual's ability to benefit from services, an individual's income or financial position, their success in applications for jobs or courses).

Example:

An employer uses aptitude tests as part of its selection process. The tests are automated and, using candidates' responses to a number of questions, generate reports indicating the personality attributes of the candidates. The organisation decides whether or not to interview people based solely on the results of such tests.

This decision has a "similarly significant effect" on individuals since it affects whether or not they are considered for a job.

Example:

A Fintech platform tracks consumers spending habits online in order to build a profile of them which it then uses to make recommendations to its customers (banks) around the financial products which might best suit the consumer, as well as giving them a rating as to their potential value as a customer. This may have a "similarly significant effect" as it could affect the financial products which the individual has access to, or the price at which the individual has access to those products.

10.2 When does the right not apply?

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 does not apply if one of the following criteria is met:

- the decision is **necessary for entering into or performing a contract** with the data subject
    - the contract does not have to be between your organisation and the data subject;
    - you must be satisfied the decision is necessary (it does not have to be essential but must be reasonable and targeted)

Example:

An individual wants to take out a loan from a specialist loan provider. The loan provider relies on a credit score which is automatically generated by a third party credit reference agency in order to decide whether to offer the individual the loan.

In this case the automated processing is a reasonable and targeted way of making the decision as to whether or not to provide the loan (and enter into the loan agreement with the individual). Even though the automated processing is carried out by another organisation, the loan provider can still rely on the "necessary for entering into a contract" exception.

- you have the **data subject's explicit consent** (see Part 1 of the Guidance, paragraph 5 for information on consent and explicit consent); or
- the decision is **required or authorised by Applicable Law** and:

- neither of the above two bullets (necessary for a contract/you have the individual's explicit consent) apply;
- you notify the data subject in writing as soon as reasonably practicable that you have made a decision based solely on automated processing; and
- within 1 month of receipt of the notification, the data subject has not asked you to reconsider or make a new decision which is not based solely on automated processing.

Example:

A financial services organisation complies with high level regulatory requirements to prevent financial crime by using decisions based solely on automated processing to identify and block potentially fraudulent money transfers.

It notifies affected data subjects of the decisions as described above.

10.3 Additional measures

If you make individual decisions based on solely automated processing because the data subject has explicitly consented or because the decision is necessary for entering into or performing a contract with the data subject, you must put in place suitable measures to safeguard individuals' rights and legitimate interests.

Section 22(3) of the DPR 2021 says that this means at a minimum enabling the individual to:

- obtain human intervention in the decision making;
- express his or her view; and
- contest the decision.

You should give individuals clear information about these measures and how they can obtain human intervention, express their views and contest the decision, for example in your privacy notice.

Making decisions based solely on automated processing, including profiling, is a high risk activity, meaning you should also carry out a data protection impact assessment before using personal data in this way. You can find out more about data protection impact assessments in Part 4 of the Guidance.

10.4 Special categories of personal data

Section 22(4) of the DPR 2021 provides an additional level of protection for special categories of personal data. If you use special categories of personal data to make decisions based solely on automated processing, you can only rely on the exceptions explained in paragraph 10.2 above if:

- you are processing the data based on the grounds in either section 7(2)(a) or section 7(2)(k) of the DPR 2021; and

- you have put in place suitable measures to protect the data subjects rights and legitimate interests.

Section 7(2)(a) applies where the data subject has given their explicit consent to the processing.

Section 7(2)(k) applies where the processing is necessary for reasons of substantial public interest. You should consult section 7(2)(k) for the full list of the public interest conditions.

The DPR 2021 do not specify minimum suitable measures to protect the data subjects rights and legitimate interests where you process special categories of personal data for automated decision making, however, you should apply at least the minimum safeguards as described in paragraph 10.3 above.

11. RESTRICTIONS ON DATA SUBJECTS' RIGHTS

Section 21 of the DPR 2021 sets out a number of restrictions on the rights described in this part of the Guidance, i.e. circumstances when particular rights do not apply. These restrictions generally relate to your purpose for processing the personal data in question. Some of the restrictions apply simply because you are processing data for the particular purpose, but most are prejudice based, i.e. they only apply to the extent to which complying with a request to exercise rights would prejudice the purpose listed in the restriction (e.g. where compliance with a request to exercise rights would prejudice national security or the prevention or detection of a crime).

You must not rely on the restrictions routinely or apply them in a blanket fashion. Instead you must consider each restriction on a case-by-case basis, taking into account the detail of the restriction itself and the processing you are carrying out.

In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance. Your organisation, as controller, is responsible for demonstrating that a particular restriction applies, if challenged.

For more information, you may contact the Commissioner of Data Protection on:

Telephone No.: 00 971 2 3338888

Email: Data.Protection@adgm.com

Address: ADGM Building, Abu Dhabi Global Market Square, Al Maryah Island, Abu Dhabi, United Arab Emirates.

Disclaimer

This Guidance is a non-binding indicative Guidance and should be read together with the Data Protection Regulations 2021 and any other relevant regulations and enabling rules, which may change over time without notice. Information in this Guidance is not to be deemed, considered or relied upon as legal advice and should not be treated as a substitute for a specific advice concerning any individual situation. Any action taken upon the information provided in this Guidance is strictly at your own risk and the Office of Data Protection, Registration Authority and ADGM will not be liable for any losses and damages in connection with the use of or reliance on information provided in this Guidance. The Office of Data Protection, Registration Authority and ADGM make no representations as to the accuracy, completeness, correctness or suitability of any information provided in this Guidance.