ABU DHABI GLOBAL MARKET

Office of Data Protection

Appropriate Policy Document

Guidance & Template

1. INTRODUCTION TO THIS GUIDANCE

Introduction to Abu Dhabi Global Market

Abu Dhabi Global Market (ADGM) is a broad based international financial centre, established pursuant to Abu Dhabi Law No. 4 of 2013 in the Emirate of Abu Dhabi. With its own civil and commercial laws based on the English common law, ADGM offers the local, regional and international business community a world-class legal system and regulatory regime.

About this guidance

This guidance is prepared to support Controllers and Processors in complying with the applicable provisions in the ADGM Data Protection Regulations 2021 (DPR 2021) regarding the processing of specific categories of sensitive data, also referred to as 'special categories of data.' The DPR 2021 requires ADGM Licensed Persons to establish a separate policy document known as an 'Appropriate Policy Document' ("APD") in cases where a Controller processes certain special categories of personal data.

Who the guidance is aimed at

This guidance applies to ADGM Licensed Persons who collects and processes special category of personal data and has day-to-day responsibility for personal data. It is aimed at small and medium enterprises although it may also be useful for larger organisations and their legal advisors.

Further details are available in relation to the ADGM DPR 2021 requirements in Part 1 of this Guidance.

What the guidance does

This guidance aims to explain what the APD is and how it may apply to your processing activities. This guidance includes a template to help you ask the right questions, and understand your obligation. However, the ultimate responsibility of how to do and how to justify decisions remains with the firm. This is a key principle of the DPR 2021, known as the accountability principle.

What are special categories of personal data?

Certain types of personal data, known as special categories or personal data, receive additional protection under the DPR 2021 because they are more sensitive. The DPR 2021 defines the following as special categories of personal data:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex** life or sexual orientation;
- personal data relating to **criminal convictions and offences or related security measures**.

NOTE: *You can only process special categories of personal data if one of the conditions set out in Article 7(2) of the DPR 2021 applies. For more information about the lawful basis for processing see Part 1 of the DPR 2021 Guidance.*

2. THE REQUIREMENT

What does the law say?

Article 7(3) of the DPR 2021 states that:

> ***Where it is specified*** *that a condition in section 7(2) is met only if the Controller has an appropriate policy document in place, the Controller will have an appropriate policy document in place if: (a) the policy document (which may incorporate other documents by reference) explains, for Personal Data Processed in reliance on the condition:*
>
> *(i) how the Controller will comply with the principles in section 4; and*
>
> *(ii) the Controller's policies regarding the retention and erasure of that Personal Data; and*
>
> *(b) from the date the Controller starts to Process Personal Data in reliance on the condition until 6 months after the Controller ceases to carry out such Processing, the policy document referred to in section 7(3)(a) is:*
>
> *(i) retained, reviewed and updated (as appropriate); and*
>
> *(ii) made available to the Commissioner of Data Protection on request.*

What specified conditions require an APD?

Section 7(2) of the DPR 2021 sets out the conditions that require Controllers to have an APD in place.

An APD is required **where the processing of special category is:**

- ✓ Necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment law.
- ✓ Necessary for reasons of substantial public interest in:
  - (i) the exercise of a function or requirement conferred on a person by Applicable Law;
  - (ii) the exercise of a function of the Board, Abu Dhabi or United Arab Emirate government;
  - (iii) the administration of justice;
  - (iv) equality of opportunity or treatment provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual; and it does not relate to an individual who has given written notice to the Controller not to Process their

Personal Data;

- (v) diversity at senior levels of organisations, where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject and is not aware of the Data Subject withholding Consent provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual;

- (vi) the prevention or detection of an unlawful act or omission where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose; and if the Processing relates to the disclosure of Personal Data to a relevant public authority;

- (vii) the protection of the members of the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a company, body or association, or failures in services provided by a company, body or association where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose;

- (viii) compliance with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or omission, or been involved in dishonesty, malpractice or other seriously improper conduct where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject to the Processing;

- (ix) the prevention of fraud in connection with Processing of Personal Data as a member of, or in accordance with arrangements made by, an antifraud organisation;

- (x) the disclosure in good faith to an appropriate public authority regarding suspected terrorist financing, to identify terrorist property or in relation to suspected money laundering, in accordance with Applicable Law;

- (xi) the publication of a judgment or other decision of a court or tribunal or if the Processing is necessary for the purposes of publishing such a judgment or decision.

What about the other conditions?

An APD **is not** required in all instances where there is processing of special category of personal data. Where the condition does not specify a need for an APD, you do not need one. You may still choose to develop one for your own governance and record-keeping.

How does this differ from the mandatory Record of Processing Activity (RoPA)?

The ADP complements the mandatory register of processing activity. The record of processing encompasses and captures **all** processing activities within your organisation. The RoPA activity would be useful in identifying those special category data covered by the above requirement for an APD. The APD is a standalone policy that is required for demonstrating accountability. The APD must be made available to data subjects and the Office of Data Protection.

3. APPROPRIATE POLICY DOCUMENT TEMPLATE

Please note, the APD does not have to be structured as per below template. The below template is intended as guideline only. You may use your own process and documentation to demonstrate compliance with the APD requirement of Article 7(3). Your APD document can include more than one activity.

1. Description of the Processing Activity

List out the special category of personal data used and the purpose for processing that information. You may wish to refer to your Record of Processing Activity for that information.

Key	Special Category of Personal Data	Purpose for Processing
1	**Example:** Physical Health Data	In order to facilitate a UAE employment visa as per UAE Immigration Laws and Regulations. Prospective employees must provide a negative result for HIV and Tuberculosis.
2		

2. Lawful Basis for Processing Personal Data

In order to process personal data, Controllers must identify and rely upon appropriate lawful basis for processing. For personal data, you must meet a condition in Article 5 of the DPR 2021. For special category of data, you also require a condition in Article 7 of the DPR 2021. For more information, please refer to Part 1 of the DPR 2021 Guidance available here: https://www.adgm.com/operating-in-adgm/office-of-data-protection/guidance

You may also wish hyperlink to your website privacy policy, internal policies and other documentation.

#	Article 5 Condition		Article 7 Condition		Link to other Documents/Policies (Optional)
	Condition	Description	Condition	Description	
1	Article 5(1)(c)	Processing is necessary for compliance with a legal obligation to which the Controller is subject under Applicable Law.	Article 7(2)(b)	Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment law	Website Privacy Policy

3. Compliance with the Principles

You should will to explain how the activities comply with the principles of processing personal data. As a Controller, you are responsible for demonstrating that your policies and procedures ensure your compliance with the DPR 2021 and in particular the principles.

Where appropriate, you may answer the below with links, references, documentations and copies of relevant policies, procedures and guidelines. You may also refer to your privacy notices. Please note, the below is not intended for you to recreate existing information. The purpose is to help you describe how you satisfy each principle. **The questions listed below are a guide in order to support you in your decision making process. The questions are not exhaustive and is only intended to act as a guide.**

Relevant provision: Article 7(3)(a)(i)

(a) Fairness, Lawfulness and Transparency (Article 4(1)(a))

Activity No #1
Activity No #2

Have we identified our lawful basis for processing?
Are we transparent with our processing of personal data with individuals?
Do we publish or make available our processing activities?
Are we clear and open regarding why we collect and process personal data?
Would a reasonable person be surprised we conduct this activity?

For more information about this Principle, you can refer to Part 1 of the DPR 2021 Guidance.

Demonstrating Accountability

We can demonstrate compliance with the above Principle for the processing activity?
We have a Transparency Notice / Privacy Policy? If staff, do we have an internal notice?
We have procedures in place?
We educate staff and provide Guidance on the processing of personal data?
Is our lawful basis 'legal obligation'? If so, do we provide clear reference(s) to the applicable legislation?
This lawful basis of this activity is included in the RoPA

(b) Purpose Limitation (Article 4(1)(b))

Activity No #1
Activity No #2

Have we identified our purpose for processing?
Have we ensured that any new purpose are compatible with the original purpose?
Are the purpose(s) clearly included in our privacy notice to individuals?

For more information about this Principle, you can refer to Part 1 of the DPR 2021 Guidance.

Demonstrating Accountability

We can demonstrate compliance with the above Principle for #1 processing activity
We have appropriate controls in place for ensuing purpose limitation;
We educate staff and provide Guidance on the processing of personal data?
If the purpose are based in Law, we provide clear reference(s) to the applicable Law.
This purpose for processing regarding this activity is included in the RoPA

(c) Data minimisation (Article 4(1)(c))

Activity No #1
Activity No #2

We only collect personal data we actually need for our specified purposes.
We have sufficient personal data to properly fulfil those purposes.
We periodically review the data we hold, and delete anything we don't need.
We have communicated to individual(s) why we require the information?

For more information about this Principle, you can refer to Part 1 of the DPR 2021 Guidance.

Demonstrating Accountability

We can demonstrate compliance with the above Principle for #1 processing activity
We have relevant policies and procedures in place
We educate staff and provide Guidance on data minimisation

(d) Accuracy (Article 4(1)(d))

Activity No #1
Activity No #2

We ensure the accuracy of any personal data we create.
We have measures in place to correct inaccuracies

For more information about this Principle, you can refer to Part 1 of the DPR 2021 Guidance.

Demonstrating Accountability

We can demonstrate compliance with this Principle for #1 processing activity
We have appropriate processes in place to check the accuracy of the data we collect
We record the source of that data alongside key information (dates/time etc).

We keep a note of any challenges to the accuracy of the personal data
We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

(e) Storage Limitation (Article 4(1)(f))

Activity No #1
Activity No #2

We know what personal data we hold and why we need it
We carefully consider and can justify how long we keep personal data
We regularly review the information we retain in line with the purpose(s) for processing
We erase or anonymise personal data when we no longer need it
We have appropriate processes in place to comply with individuals' requests for erasure

Demonstrating Accountability

We can demonstrate compliance with this Principle for #1 processing activity
We have a retention policy and schedule in place?
We have demonstrable processes in place for deleting/destroying information after its retention period expires?
We educate staff and provide Guidance on retention?
We can demonstrate our processes for complying with individual rights requests.
The retention for this activity is included in the RoPA

(f) Security (Article 4(1)(g))

Activity No #1
Activity No #2

We have appropriate technical and organisational measures in place to protect personal data
We regularly assess the security of our controls for our processing activity
We have a process and procedures in place to respond to a breach of personal data
We ensure we have appropriate contractual safeguards in place with third party Processors

Demonstrating Accountability

We can demonstrate the effectiveness of our security controls for #1 processing activity
We have appropriate Information Security Policy and Procedures in place
We educate staff and provide Guidance on Security
We have a personal data breach response process for managing incidents
We conduct regular assessments &/or stress testing (including audits) on our technical and organisational measures in place

4. Retention Policy

You must explain your policies regarding the retention of personal data for each of the processing activities.

You may refer to existing retention policies and procedures. You may also refer to the accountability measures in your response above to the Storage Limitation principle of Article 4(1)(f). In any case you must explicitly list out the retention period for the processing activities.

Relevant provision: Article 7(3)(a)(ii)

5. Review Date

You must review your APD and ensure it is kept up to date.

Relevant provision: Article 7(3)(b)(i)

Review Date: Click here to enter a date.

Version Control: v 1.0

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.