ABU DHABI GLOBAL MARKET

# Guidance on the Data Protection Regulations 2021

## Part 7:

- Codes of Conduct
- Role of Office / Commissioner of Data Protection

## Office of Data Protection

## TABLE OF CONTENTS

# 1. INTRODUCTION

## Introduction to this Guidance

**1.1** This is Part 7 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). It covers the following topics:

- Codes of Conduct (see paragraph 2); and
- Role of Office/Commissioner of Data Protection (see paragraph 3).

# 2. CODES OF CONDUCT

## 2.1 What are codes of conduct?

Codes of conduct are voluntary accountability tools which organisations can elect to adhere to, enabling associates and other bodies representing categories of controllers or processors to identify and resolve data protection challenges which commonly arise in their sector with assurance from Commissioner that the code, and its monitoring, is appropriate.

A code of conduct might be developed by:

- an association/consortium of associations or other bodies representing categories of controllers or processors;
- a sectoral organisation;
- trade or representative associations;
- academic associations; or
- interest groups.

They can help you to reflect on your processing activities and ensure you follow rules designed for your sector to achieve good practice. They are written by an organisation or association representing a sector in a way that controllers and processors operating in that sector understand and enable sectors to provide solutions to common issues with advice and support from the Commissioner.

By signing up to a code of conduct, controllers and processors can ensure they apply the DPR 2021 effectively and in doing so establish standard compliance practices that ultimately should assist in bringing down levels of non-compliance with the DPR 2021.

## 2.2 Why sign up to a code of conduct?

Adhering to a code of conduct shows that you:

- follow the requirements for data protection that have been agreed by the Commissioner as representing good practice within your sector or category; and
- are appropriately addressing the type of processing activities you are undertaking and the related level of risk. For example, a code may contain specific sectoral requirements when it relates to processing of sensitive special category personal data.

Adhering to a code of conduct could help you to:

- demonstrate, as controller, that you have implemented appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the DPR 2021;

- demonstrate, as a processor or a sub-processor, that you provide sufficient guarantees where processing personal data on behalf of a controller (or another processor), as referred to in sections 26(1) and 26(5) of the DPR 2021;

- demonstrate that you have considered the measures which you have taken to protect the rights of individuals in the context of the processing activities you perform (which may be similar to those of others in your industry) and that those measures are aligned with best practice in your sector such as, for example, pseudonymising personal data which does not need to be fully identifiable for the purpose for which you are processing it;

- assess the impact of your processing activities on data subjects, in particular for the purposes of performing Data Protection Impact Assessments;

- be more transparent around your processing activities (for example, by communicating privacy notices in line with the specific requirements developed under a code of conduct);

- promote confidence in a sector as a whole by creating effective safeguards to mitigate the risk around processing activities;

- earn the trust and confidence of data subjects and promote their rights, encouraging them to exercise those rights and making such exercise as straightforward as possible;

- develop a clear and comprehensive approach to breach notification and privacy by design; and

- improve the understanding within your organisation around what compliance with the DPR 2021 means in the context of your sector.

## 2.3 What should a code of conduct address?

Codes of conduct should serve to help you to comply with the DPR 2021. They should cover the requirements of the DPR 2021 and should give careful consideration to how those requirements apply in the context of the sector in which you operate.

A code of conduct should provide a valuable point of reference to a sector and should cut costs for businesses in the sector seeking to comply with the DPR 2021 by contextualising the requirements of the law, allowing them to take steps towards compliance in an efficient and cost effective manner.

## 2.4 Who is responsible for codes of conduct?

Trade associations or bodies who are able to speak on behalf of controllers or processors can create a code of conduct. It is recommended that codes of conduct are developed in consultation with relevant stakeholders, such as controllers or processors in the ADGM, the businesses they interact with (e.g. their IT suppliers) and even including members of the public. Where a code of conduct has been developed in another territory (such as the UK), it could be leveraged and adjusted for use in the ADGM (subject to approval from the Commissioner).

We will:

- provide advice and guidance to bodies considering or developing a code;
- check that codes meet the code criteria set out below;
- approve and publish codes of conduct; and
- maintain a public register of all approved codes of conduct.

## 2.5 How will the Commissioner approve a code of conduct?

All codes of conduct received will be assessed against the following criteria to ensure that the code submission meets the following requirements:

- outlines the code owner's ability to represent controllers or processors covered by the code. The code owner must be able to demonstrate that they are able to speak on behalf of a group of organisations, have the necessary experience within their sector and understand the needs of the organisations to which the code applies.
- includes a concise statement explaining the purpose of the code, the benefits to members and how it effectively applies the DPR 2021.
- identifies processing operations that the code covers and the categories of controllers or processors that it applies to as well as what the data protection issues are that it intends to address.
- outlines the stakeholder consultation which took place in the course of preparing the code and outcomes of the consultation; and
- complies with other relevant ADGM legislation, where required.

We would recommend engaging with the Commissioner during the development stage of your code of conduct, prior to any formal submission, to ensure that when drafting the code, you are meeting the necessary criteria and understand the requirements of the DPR 2021. The Commissioner can be contacted using the contact details provided at the end of this document.

Upon receiving a submission for a code of conduct, the Commissioner may make recommendations for improvement before proceeding to approve the code of conduct (if it meets the Commissioner's requirements) or rejecting it (if it still does not). It may also seek opinions from other authorities.

## 2.6 How will compliance with the code be monitored?

The Commissioner will monitor compliance using various methods. This may include exercising his powers under the DPR 2021 through auditing or ad-hoc inspections. Code owners and entities seeking to be rely on codes of conduct must be regulated by the ADGM and the Commissioner. Compliance may also be enforced through standard contractual provisions to ensure monitoring bodies are overseeing their members' compliance in the case of trade association bodies. Any contractual provisions will be without prejudice to the Commissioner's powers to enforce and regulate the DPR 2021.

### 2.7 What are the practical implications for our organisation?

- You can sign up to a code of conduct relevant to your data processing activities or sector. You can sign up to more than one code of conduct, provided that it is relevant to your processing activities or sectors.

- Your customers will be able to view your code membership via the code's webpage and the ADGM's public register of Commissioner approved codes of conduct.

- Once you are assessed as adhering to the code, your compliance with the code should be monitored on a regular basis (either by your DPO or by a Commissioner approved code owner). Your membership can be withdrawn if you no longer meet the requirements of the code.

- When contracting work to third parties, you may wish to consider whether they have signed up to a code of conduct, as part of meeting your due diligence requirements when appointing a third party processor under the DPR 2021.

### 2.8 How do we sign up to become a code member?

As at the date of publication of this guidance, the Commissioner has not yet formally approved any codes of conduct. You may wish to contact your trade association/representative body or a body able to legitimately speak on your behalf to discuss whether they are developing a code in your sector.

The Commissioner welcomes enquiries from organisations who are considering writing, monitoring or signing up to a code of conduct.

### 2.9 Will the ADGM publish approved codes of conduct on its website?

Yes. The Office of Data Protection will register and publish ADGM codes approved by the Commissioner on our website, including the name of code owner, the code title, sector, and the date and version of the code that the Commissioner has approved.

The Commissioner will also publish details of entities that adhere to the code of conduct.

### 2.10 Are cross-sector codes permitted?

Yes. Cross-sector codes are possible (for example, IT professionals working across multiple industries) if the code owner can demonstrate that the organisations covered have a common processing activity and share the same processing needs. In these circumstances suitable organisations such as a HR professional body or IT association would need to develop the code, as opposed to a sector specific organisation.

## 3. ROLE OF OFFICE / COMMISSIONER OF DATA PROTECTION

### 3.1 What is the role of the Commissioner of Data Protection?

The Commissioner of Data Protection is the head of the Office of Data Protection. The Commissioner is ultimately responsible for the monitoring and enforcing the application of the DPR 2021 in order to protect the rights of natural persons in relation to processing of personal data in the ADGM.

The Commissioner is required by law to remain independent and free from external influence when performing his duties.

### 3.2 What is the role of the Office of Data Protection?

The Commissioner of Data Protection performs his functions with the support of the Office of Data Protection. Those functions include the following:

- exercising investigative powers, where necessary (see paragraph 3.3 below);
- monitoring and enforcing the application of the DPR 2021 (see paragraph 3.4 below);
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;
- advising and issuing opinions to the ADGM Board of Directors, Registration Authority, Financial Services Regulatory Authority, ADGM Courts, and other institutions and bodies on legislative and administrative measures relating to the protection individuals rights with regard to the processing of personal data;
- promoting the awareness of controllers and processors of their obligations under the DPR 2021. One way in which we achieve this is by publishing this Guidance. The Commissioner of Data Protection may also engage in outreach programmes to raise awareness and increase understanding of the DPR 2021;
- providing the public with opportunities to provide views on the activities of the Office of Data Protection;
- handling complaints lodged by individuals, and investigating, to the extent appropriate, the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation is necessary;
- cooperating with, including sharing information and provide mutual assistance to, other data protection authorities with a view to facilitating the effective enforcement of legislation for the protection of personal data worldwide. Given the ADGM's status as a global financial hub, it is key that it is aligned with international best practice and participate on an international level in the improvement of data protection compliance;
- monitoring relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and business practices;
- adopting standard contractual clauses (as per sections 26(6) and 42(2) of the DPR 2021);
- publishing and maintaining a list as to the types of processing operations which typically required a data protection impact assessment (as per section 34(4) of the DPR 2021);
- approving codes of conduct and certification criteria (as per sections 38(1) and 39(1) of the DPR 2021);
- authorising contractual clauses and provisions referred to in section 42(4) of the DPR 2021;
- approving binding corporate rules pursuant to section 43 of the DPR 2021;
- issuing guidance and publishing standard forms;

- keeping records of non-compliance by those entities caught by the DPR 2021, as well as any measures taken as a result of such non-compliance; and

- collecting data protection fees and renewal fees.

### 3.3 Investigative powers

The Commissioner has broad investigative powers under the DPR 2021. Those include the power to:

- order, by notice in writing, controllers and processors to provide any information it reasonably requires for the performance of its duties and functions;

- initiate investigations into a controller's or processor's compliance with the DPR 2021. This could include both requesting information from you and physically attending your offices. We also have the power to access any equipment used to process personal data (such as computers) and to take possession of any relevant documentation or information. We must give you written notice of the decision to investigate unless the Commissioner believes that would likely result in the investigation being frustrated;

- carry out investigations in the form of data protection audits;

- carry out a review on certifications issued pursuant to section 39 of the DPR 2021;

- notify controllers and processors of any alleged contravention of the DPR 2021; and

- obtain, by notice in writing, from controllers and processors, access to all personal data and to all information reasonably necessary for the performance of its duties and functions. This could mean you granting us access to your IT systems.

### 3.4 Enforcement powers

The Commissioner has the power to:

- issue and publish directions and warnings and make recommendations to controllers and processors that intended processing operations are likely to contravene provisions of the DPR 2021;

- issue and publish directions and reprimands to controllers and processors where processing operations have already contravened provisions of the DPR 2021. This could be, for example, where we become aware that you are transferring personal data internationally without a legal basis to do so under the DPR 2021;

- order controllers and processors to comply with an individual's requests to exercise his or her rights pursuant to the DPR 2021. For example, if you have refused to honour a data subject's right to erasure, the Commissioner may compel you to do so (where the individual has that right under the DPR 2021);

- order controllers and processors to bring processing operations into compliance with the provisions of the DPR 2021, where appropriate, in a specified manner and within a specified period. For example, if you have not issued a privacy notice which meets the requirements of the DPR 2021 to a certain category of data subjects (such as your

employees), the Commissioner may instruct you to do so within a certain period of time, or risk a fine;

- order a controller to communicate a personal data breach to the individual, where it has not done so already;

- impose a temporary or permanent limitation (including a ban) on processing;

- order the rectification or erasure of personal data or restriction of processing pursuant to sections 14, 15 and 16 of the DPR 2021 and the notification of such actions to Recipients to whom the personal data has been disclosed, pursuant to sections 15(2) and 17 of the DPR 2021;

- withdraw a certification if the requirements for the certification are not or are no longer met;

- impose an administrative fine pursuant to section 55 of the DPR 2021, in addition to, or instead of, any of the other measures set out under the DPR (as summarised in this paragraph 3.4). When considering whether to issue a fine the Commissioner will consider the circumstances on a case by case basis. For particularly serious breaches the Commissioner may well issue a fine and issue an order for you to resolve your infringement moving forwards;

- order the suspension of data flows to a recipient inside or outside of ADGM or to an international organisation; and

- where appropriate, refer contraventions of the DPR 2021 to the attention of the court and where appropriate, commence legal proceedings, in order to enforce the provisions of the DPR 2021.

### 3.5 What does the Commissioner not do?

The Commissioner is not competent to supervise data processing operations of the ADGM Courts acting in its judicial capacity.

The Commissioner does not give legal advice or advise on issues specific to particular processing activities, including the regulatory risks associated with the various approaches to those processing activities (other than in the context of data protection impact assessments, as explained in Part 4 of this Guidance).

## 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.