ABU DHABI GLOBAL MARKET

OVERVIEW OF THE ADGM DATA PROTECTION REGULATIONS 2021

Introduction

The Abu Dhabi Global Market (ADGM), an international financial free zone in Abu Dhabi, enacted the new ADGM Data Protection Regulations 2021 on the 11th of February 2021. The new Regulations repeal the existing Data Protection Regulations 2015 and mandate additional obligations and responsibilities for entities that process personal data.

What do the updated Regulations entail?

The updated Regulations are a new chapter in the ADGM's long-standing commitment to globally recognized standards of data protection.

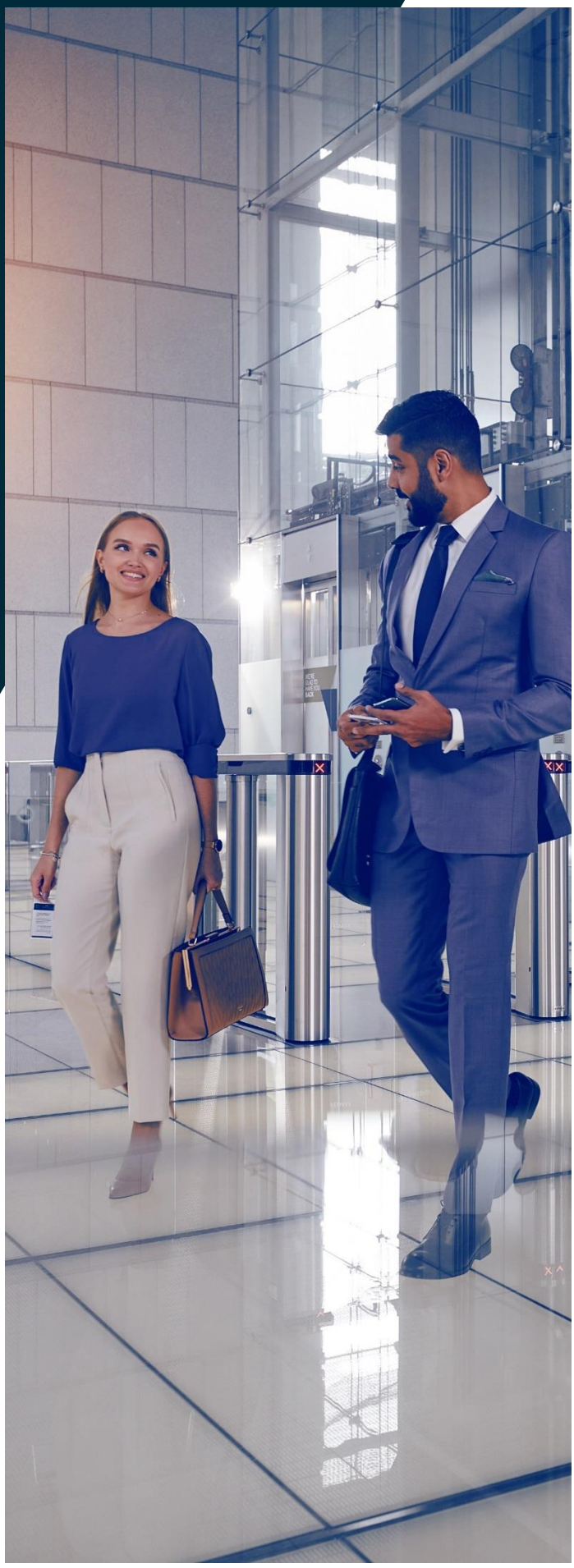
The goal is to establish enhanced governance and transparency requirements that will facilitate the ADGM's alignment with international laws and Regulations.

When do the Regulations come into effect?

For new entities incorporated on or after the 14th February 2021, the new Regulations come into effect on the 14th August 2021. For existing entities, the Regulations will come into effect on the 14th February 2022.

Who is affected by the new Regulations?

The new Regulations apply to all entities established in the ADGM. If your entity is processing personal data, or processing in the context of the activities of an establishment in the ADGM, the new Regulations apply. Personal data is defined broadly in the new Regulations and covers any information that can identify a living person (i.e. a Data Subject).



What are the advantages of new Regulations?

- Aligns ADGM with a globally accepted approach to data protection.
- Promotes consistency and interoperability with international best practice
- Underpinned by a common law legal framework through the ADGM Courts.
- Provides a safe and secure ecosystem for the protection of personal data
- Establishes an independent Office of Data Protection and equips it with effective powers to regulate the Regulations

What are the key provisions of the Regulations?

General Requirements

Personal data processing principles	Requires Controllers to comply with the Principles which include using personal data lawfully, fairly and transparently.
Individual Rights	Provides individual with rights and obligates entities to implement appropriate measures to identify, record and manage requests.
Data Processing Agreement	Requires Controllers to identify entities processing personal data on their behalf and mandatng the use of Data Processing Agreements.
Data Transfers	Identify transfers including access to personal data outside of ADGM to third parties. Exporters must rely upon a suitable condition or mechanism under the Regulations to transfer Personal data.
Data Protection Impact Assessment (DPIA)	Perform DPIAs for high-risk processing activities.
Security of Processing	Implement appropriate security controls to ensure ongoing confidentiality, integrity, and availability of personal data.
Accountability	All entities must be able to demonstrate compliance with the Regulations

Key Data Subject Rights

Right to transparent information and communication

Individuals have the right to concise, transparent information, provided in an easily accessible form.

Right to be informed

Individuals have the right to be informed about the collection and use of their information.

Right to request access and rectification

Individuals have the right to request a copy their personal data and/or request rectification of inaccurate information.

Right to object to processing

Individuals have the right to object to processing of their data. For marketing, this is an absolute right.

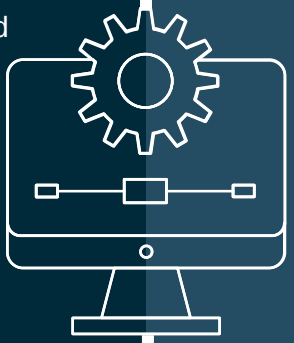
Right to request deletion

Individuals have the right to request the deletion of their data in certain circumstances.

Key Data Controller and Data Processor Obligations

Controller:

- Ensure compliance with the Principles and Data Subject Rights.
- Implement appropriate technical and organizational measures to demonstrate compliance.
- Enforce data protection by design and by default
- Maintain records of processing activities
- Ensure on-time payments of data protection fee to the Commissioner of Data Protection
- Notify the Commissioner of Data Protection of personal data breaches within the required timelines



Processor:

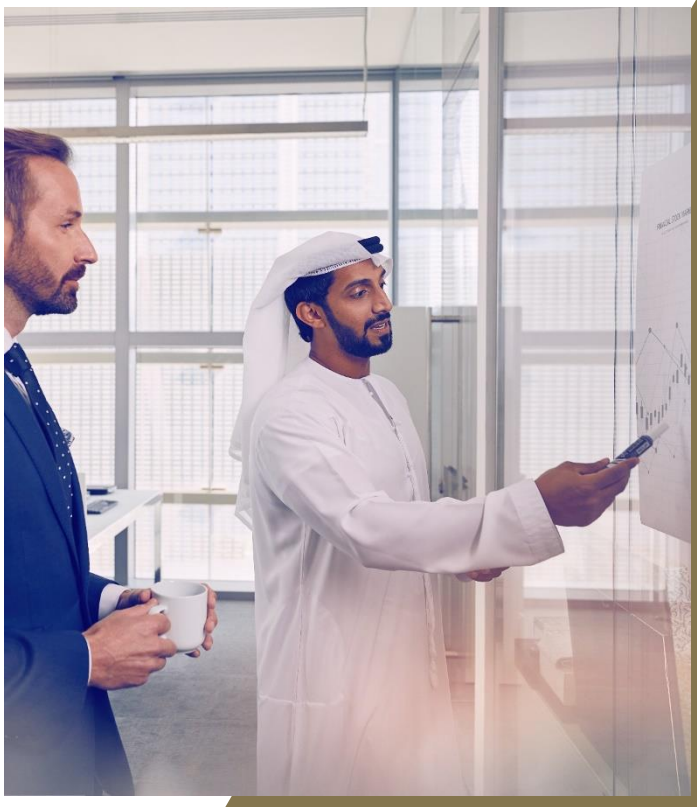
- Process personal data only on documented instructions from the Controller
- Ensure confidentiality while processing personal data
- Assist the Controller in implementing appropriate technical and organizational measures and providing required information for processing
- Return all personal data to the Controller after the end of the provision of services relating to processing

Data Protection Officer

For certain entity types it may be mandatory to appoint a Data Protection Officer (DPO).

The DPO is:

- an expert advisor in Data Protection Laws and Practices;
- tasked with monitoring compliance and performing assessments;
- required to act as the contact point for individuals and the ADGM Office of Data Protection on issues relating to processing;
- bound by secrecy or confidentiality concerning the performance of the tasks, in accordance with applicable law and the confidentiality policies and procedures of the Controller or Processor.



Data Protection by Design and Default

Data Protection by Design and Default is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product, or process and then throughout its implementation and operation, including any updates or expansion, and at its ultimate termination, closure, or migration.

Data Protection by Design and Default must be considered throughout the lifecycle of a processing activity or processing system: at development, design, and at the point of processing.

Ways in which Data Protection by Design and Default might be implemented include:

- Putting in place appropriate technical and organizational measures designed to implement the data protection principles.
- Building safeguards into your processing activities so that you meet the requirements of the DPR 2021 and protect individual rights.

Fundamental Principles of Data Protection by Design and Default

01 Data Protection should be embedded into system and process design from the inception

02 Data Protection requirements should be considered proactively, not reactively

03 Data Protection should be configured as the default setting, without requiring user intervention

04 Data Protection should consider the security of data end-to-end, from creation to destruction or archival

05 Data Protection should be “Full functionality Positive-sum” and should incorporate all privacy and security objectives

06 Data Protection should be user-centric and should provide individuals with control over their data

07 Data Protection should be managed with visibility and transparency towards individuals

Transferring and Sharing of Data Outside of ADGM

Personal Data should not be transferred outside of ADGM without appropriate safeguards. There are three mechanisms of transfers:

1. **Adequacy**: The recipient is located in a jurisdiction that provides an adequate level of protection. The list of adequate jurisdictions is on the ADGM ODP website
2. **Appropriate Safeguards:** The exporter can rely upon suitable safeguards to transfer personal data. In particular, ADGM-approved Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).
3. **Derogation:** The exporter could transfer personal data if certain conditions exist. The conditions are as follows:

> *Transfer provisions exist in the Regulations to allow the free flow of personal data outside of ADGM. The purpose of these conditions is to ensure data is given an appropriate level of protection irrespective of the destination.*

- ✓ Consent of the individual is provided for the transfer
- ✓ Necessary for the performance of a contract between an individual and the Controller
- ✓ Necessary for the conclusion or performance of a contract
- ✓ Necessary for important reasons of public interest in ADGM
- ✓ Required by law enforcement agencies of the UAE
- ✓ Necessary to protect a person's life
- ✓ For the exercise or defense of legal claims
- ✓ Necessary to comply with certain specific regulatory requirements

The Office of Data Protection has developed some templates for standard contractual clauses (SCCs) which are provided as part of the guidance available on the ADGM ODP website. These templates meet the requirements of Article 26(3).

Commissioner of Data Protection

Key Responsibilities

The Commissioner of Data Protection is appointed by the Board of Directors of ADGM to administer the Regulations. The Office of Data Protection is the independent supervisory authority of the ADGM. The Data Protection Regulations assign responsibilities to the Commissioner of Data Protection, some of which are listed below.

The responsibilities of the Commissioner of Data Protection include:

Education and Advisory

Provide guidance on the ADGM Data Protection Regulations to Controllers, Processors, and to the wider public.

Monitoring and Enforcement

Monitor compliance with the ADGM Data Protection Regulations and enforce its provisions.

Handling and Investigating Complaints

Handle complaints and breaches of the ADGM Data Protection Regulations.

Legislative Advisory

Advise on new or proposed legislations that impact individual rights and the processing of personal data.

Promote Public Awareness

Promote public awareness and understanding of the risks, rules and safeguards in relation to data processing.

Authorize Cross Border Data Transfers

Issue Adequacy Decisions and approve transfer mechanisms in accordance with the ADGM Data Protection Regulations.