ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

Privacy Accountability

Thematic Review – March 2019

ADGM Office of Data Protection

CONTENTS

Executive Summary 2

Chapter 1 – Introduction 3

Abu Dhabi Global Market 3

Registration Authority 3

The Office of Data Protection 3

Chapter 2 – Background, Scope and Approach 4

Background 4

The 2018 GPEN Privacy Sweep ("the Sweep") 4

Why did ADGM participate in the Sweep? 5

Who will be interested in this report? 6

Scope 6

Approach 8

Chapter 3 – The Results 10

General Findings 10

Findings by Indicator 11

Good Practices 16

Chapter 4 – Conclusions and Next Steps 17

Conclusions 17

What does ADGM want to achieve? 17

What happens next? 17

Executive Summary

ADGM's Office of Data Protection is the data protection supervisor of the ADGM and is a member of the Global Privacy Enforcement Network (GPEN), a global network of privacy supervisory authorities.

In September 2018, the Office of Data Protection conducted a privacy review of entities registered in ADGM, as part of its participation in an annual review conducted by GPEN members globally, known as the GPEN Privacy Sweep. This report explains the review methodology, results and next steps.

The objectives of the review included to raise awareness of and encourage compliance with ADGM's privacy regime, and to identify areas requiring attention as well as best practices among the entities.

The theme of the review was *Privacy Accountability*. Privacy Accountability is a regulatory principle concerning an organisation taking responsibility for privacy by implementing effective privacy programs, maintaining compliance with those programs and being able to demonstrate that it is doing both.

The review focused on assessing how well ADGM entities have implemented accountability into their own internal privacy programs and policies. To do so, a framework consisting of the following five (5) indicators was used:

1. **Policies, procedures and governance;**
2. **Monitoring, training and awareness;**
3. **Transparency;**
4. **Responsiveness and incident management; and**
5. **Risk assessment, documentation and data flows.**

Thirty-one (31) entities were selected for the review, sixteen (16) financial and fifteen (15) professional services, who were each requested to complete a questionnaire covering the five privacy accountability indicators. Each firm's responses were reviewed and assigned a rating, of '*very good*', '*satisfactory*' or '*poor*' by the Office of Data Protection.

In terms of results, the majority of entities reviewed have internal privacy policies in place or in process and a person responsible for data protection. However, improvement is needed on implementing and/or making accessible privacy policies to customers and the public. The areas of staff training and data breach handling also require attention.

Whether the entity was a financial or professional services firm made little difference to the results, but there was a difference between small and large entities, with larger entities generally performing better.

The Office of Data Protection will use this information to focus its education and outreach efforts specifically on the need for staff training, privacy policies and data breach handling, particularly for small to medium sized entities, with the aim of improving these aspects.

Chapter 1 – Introduction

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 Common law, ADGM offers the local, regional and international business community a world-class legal system and regulatory regime.

Registration Authority

The Registration Authority is one of ADGM's three independent authorities, together with the Financial Services Regulatory Authority and ADGM Courts. The Registration Authority is responsible for the registration and commercial licensing of businesses operating in or from the ADGM located on Al Maryah Island, Abu Dhabi.

The Registration Authority is also responsible for monitoring compliance with and, where necessary, enforcing the requirements under ADGM's commercial legislation.

The Office of Data Protection

The ADGM Office of Data Protection is the data protection supervisor for the ADGM. Established by decision of the ADGM Board of Directors in December 2017, the Office of Data Protection's role is to administer the ADGM's data protection regime (the Data Protection Regulations 2015 (as amended)), including maintaining a register of Data Controllers, enforcing the obligations upon Data Controllers and upholding the privacy rights of individuals as set out under the regime.

The Office of Data Protection also provides guidance to ADGM licensed persons and receives complaints from individuals.

For more information and data protection resources, please go to the Office of Data Protection micro-site available from the ADGM website at: www.adgm.com

For further information or enquiries please contact us via email at: Data.Protection@adgm.com

Chapter 2 – Background, Scope and Approach

Background

Between September and October 2018, the ADGM Office of Data Protection undertook a review of entities registered in ADGM on the theme of privacy accountability as part of its participation in the GPEN Privacy Sweep, as detailed in this report.

GPEN and the Privacy Sweep

GPEN is a global network of privacy enforcement authorities established in 2010 to promote and support cooperation in cross-border enforcement of laws protecting privacy. Currently GPEN has more than 64 members from over 47 jurisdictions. ADGM is the only GPEN member in the Arabian Gulf region.

The GPEN Privacy Sweep is an annual initiative aimed at increasing awareness of privacy rights and responsibilities, encouraging compliance with privacy legislation and enhancing co-operation between international privacy enforcement authorities.

Each year, GPEN selects a theme to study such as the collection of personal information, how it is being used, how it is protected and to whom it may be disclosed. GPEN members around the world conduct the review in their jurisdictions and then collaborate on the findings. Conclusions on best practices and methods for how organizations can improve privacy protections are compiled and made public.

The 2018 GPEN Privacy Sweep ("the Sweep")

2018 marked the sixth edition of the Sweep and the theme was Privacy Accountability.

Participating in the Sweep provided an opportunity to undertake a high level review on the extent to which ADGM entities have implemented the principle of privacy accountability across their business, and their ability to manage privacy risk in their business processes.

Why did ADGM participate in the Sweep?

As a member of GPEN, ADGM's Office of Data Protection participated in the Sweep to contribute to the coordinated effort to assess issues relating to Privacy Accountability with other member jurisdictions.

Participating in the Sweep also provided an opportunity to undertake a high level review on the extent to which ADGM entities have implemented the principle of privacy accountability across their business, and their ability to manage privacy risk in their business processes.

Participation in the Sweep also supported the Office of Data Protection's objectives by:

- **Raising awareness and encouraging compliance with privacy legislation in ADGM;**
- **Identifying opportunities, based on information revealed during the Sweep, for targeted education and/or supervisory follow up;**
- **Identifying and sharing best practices; and**
- **Facilitating future collaborative measures with other data protection authorities.**

Who will be interested in this report?

This report summarises a thematic review carried out by the ADGM Office of Data Protection on privacy accountability with thirty-one (31) ADGM licensed persons. The information provided in this report is not guidance on the operation of ADGM's data protection legislation.

This report is relevant to licensed persons in ADGM that process personal data (i.e. Data Controllers) and other persons including potential applicants, advisors and interested parties.

Scope

Privacy Accountability

In general, accountability is a common principle that relates to taking responsibility. In regulation, accountability has become a key principle in many frameworks including data protection.

Privacy Accountability is a regulatory principle concerning organisations taking responsibility for privacy by implementing effective privacy programs, maintaining compliance with those programs and being able to demonstrate that they are doing both.

The Office of Data Protection's review, as part of the Sweep, focused on assessing how well ADGM entities have implemented accountability into their own internal privacy programs and policies.

Privacy accountability was assessed based on a framework consisting of the following five (5) indicators (the "privacy accountability indicators"):

1. Policies, procedures and governance;
2. Monitoring, training and awareness;
3. Transparency;
4. Responsiveness and incident management; and
5. Risk assessment, documentation and data flows.

Guidance on the elements of each indicator is set out below (next page).

Indicator 1

Policies, procedures and governance

- Maintaining an internal privacy framework which has been embedded into everyday operations.
- Having a senior leadership post responsible for privacy and data protection.

Indicator 2

Monitoring, Training and awareness

- Delivering and maintaining an effective training and awareness programme for employees.
- Monitoring organisational performance in relation to data protection standards.

Indicator 3

Transparency

- Appropriate transparency about the organisations handling of personal data.
- Active promotion of the organisation's privacy policies to customers and third parties.

Indicator 4

Responsiveness and incident management

- Maintaining an incident management programme to mitigate the risk of a data breach.
- Having policies and procedures in place to respond appropriately to requests and complaints from individuals and other external enquiries including regulators.

Indicator 5

Risk assessment, documentation and data flows

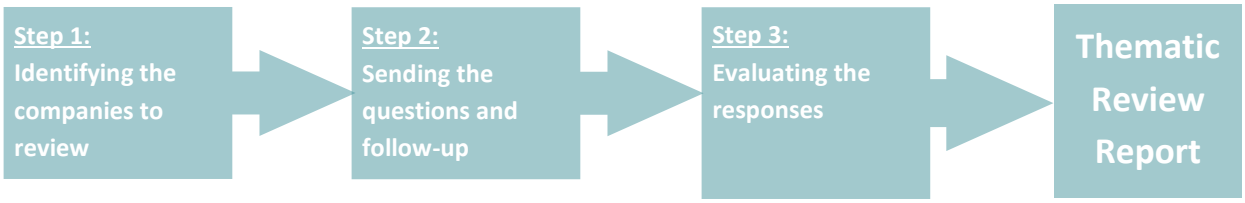
- Having processes in place to assess the risks associated with new products, services, technologies and business models.
- Maintaining records or an inventory of the organisations personal data holdings and data flows.

A range of ADGM entities of varying size and type from two sectors, financial services and professional services, were selected for the review (as detailed in the next chapter). The results set out in this report are based on the responses from those entities.

Approach

The review was conducted between September and October 2018.

The approach to conducting the review involved three main steps as set out in the diagram below.



Step 1 – Identifying the companies to review

The first step required identifying which companies to review. Whilst ADGM permits a broad range of business activities, as an international financial centre, the Office of Data Protection decided to focus on two sectors, namely, financial services and professional services, for this review.

Following that a total of thirty-one (31) entities were randomly chosen, consisting of fifteen (15) professional services entities and sixteen (16) financial services entities.

At that time 126 professional services entities were registered in ADGM, therefore 15 entities represented twelve per cent (12%) of the population. Meanwhile, with 60 financial services entities registered, the sample of 16 represented twenty seven per cent (27%) of that population of entities.

The professional services entities in the study represented a wide range of activities including accounting, auditing, legal and consultancy. The financial services entities covered both banking and capital markets activities.

In respect of the legal form of the entities in the review, there was a range of types, whereby out of 31 licensed persons, 11 were private companies limited by shares, 2 were limited liability partnerships, 9 were branches of a foreign company, 7 were branches of a limited liability partnership and 2 were branches of a foreign partnership.

Step 2 – Sending the questions and follow up

GPEN prepared a list of twelve questions covering the five privacy accountability indicators, for participating members to use in the Sweep. This ensures a consistent approach and allows for the results from each jurisdiction to be compared and to identify common themes at an international level.

The entities in the review were sent the twelve questions, which required a self-assessment response of, achieved, partially achieved or not achieved, as well as an explanation and/or evidence to support the self-assessment rating.

For the list of questions and questionnaire format, refer to **Annex A**.

Step 3 – Evaluate the responses

After following up and receiving a completed questionnaire from all the entities, the Office of Data Protection reviewed all responses. As part of the Sweep methodology, an entity's response to each of the twelve questions was assessed and assigned a rating of: *very good*, *satisfactory*, or *poor*. To ensure consistency in the evaluation, guidance on the rating criteria was issued by GPEN to participating members.

As part of its participation in the Sweep, the Office of Data Protection also provided its results to GPEN (on an anonymous basis), to be compiled into a global set of results to identify trends at an international level. ADGM's results along with a comparison of high level international findings are presented in the next chapter.

Chapter 3 – The Results

General Findings

This chapter sets out our findings from the analysis of the information provided by the entities and firstly covers general findings followed by findings by indicator, best and worst elements, as well as good practices.

Difference between the financial and professional services sectors

As noted above, the review contained entities from two sectors, professional services and financial services.

Based on the results of the review, there was no discernable difference between the two sectors. There was an equal number of financial services and professional services entities that were found to be *very good* on privacy accountability overall, just as there was an equal number rated *poor* overall.

Differences based on size and home jurisdiction

However, in general, there was a difference in results based on size and home location of entities in the review. That is, entities from larger or multi-national organisations tended to record better ratings than smaller or standalone entities across both financial and professional services.

Entities that are a member of a group headquartered in Europe, also tended to receive better ratings.

Reliance on ISO 27001 – Information Security Management Systems

Another observation was the number of entities making reference to being certified and compliant with ISO 27001[1] in order to demonstrate compliance with elements of privacy accountability. This is certainly relevant in several aspects of data protection requirements, particularly in relation to information security.

However, some entities referred to their accreditation with the standard in order to demonstrate compliance on privacy accountability indicators where the standard is not relevant.

For example, one firm referred to its information security management policies and procedures as evidence in relation to the question on whether the firm has an internal data privacy policy. Whilst related, information security management policies are not the same as a data privacy policy.

This may suggest an over reliance on the standard by entities to meet their data protection obligations.

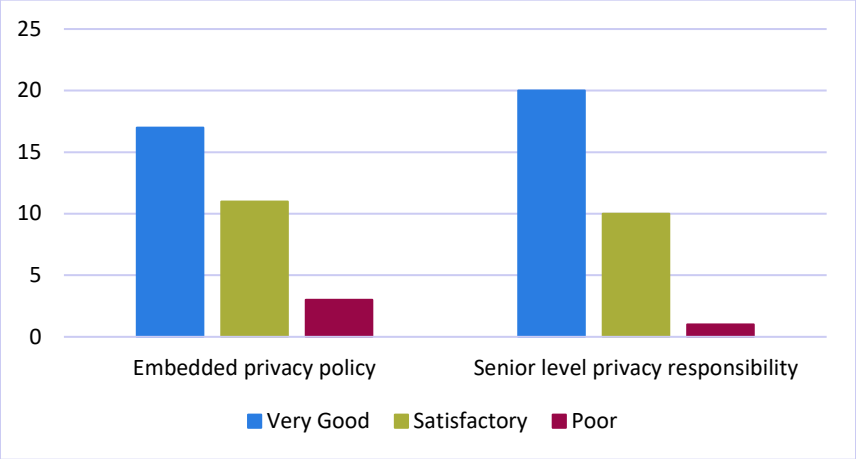
[1] The International Organisation for Standardisation's standard on Information Security Management Systems (ISMS).

Findings by Indicator

Indicator 1 – Policies, Procedures & Governance

Twenty-eight out of thirty-one entities (90%) were rated as either *very good* or *satisfactory* in respect of maintaining a privacy framework embedded into everyday practices, meaning that those entities have privacy policies in place or were in the process of implementing them. Three entities were rated as *poor* for indicating that they do not have any privacy policy nor are developing one.

Thirty out of thirty-one entities (97%) were rated as either *very good* or *satisfactory* in respect of having a person responsible for privacy and data protection at the organisation. Having a responsible person at a sufficiently senior level was required for a '*very good*' rating. Only one entity indicated that it did not have a person responsible for privacy and data protection.



Based on these results the majority of entities in the review are performing well in respect of Indicator 1.

International comparison: the results observed in ADGM on indicator 1 were largely comparable to the international findings compiled by GPEN, with the majority of entities internationally having a policy in place or in progress, as well as a large proportion of entities having appointed an individual or team responsible for compliance with data protection rules and regulations.

Indicator 2 – Monitoring, Training & Awareness

Fourteen entities (45%) were rated as *very good* on staff training by indicating that they provide initial and annual refresher training. Eleven entities (35%) indicated that they provide some kind of privacy training but it is not regular or mandatory. While six entities (19%) were rated *poor* for indicating that they do not provide any privacy or data protection training.

Eleven entities (35%) were rated as *very good* for indicating that they monitor their performance in relation to data protection standards either through self-assessments and/or annual audits. Twelve entities (39%) were rated *satisfactory* for indicating that they do conduct assessments (or are in the process of doing) but they are not regular. Eight entities (26%) do not monitor their performance on data protection.

Based on these results, the majority of entities are not performing overly well on Indicator 2.

International comparison: in respect of staff training, ADGM shared in common the finding internationally that there is significant room for improvement, particularly to ensure that refresher training is given to all staff.

Indicator 3 – Transparency

This indicator considers whether entities maintain privacy policies to explain how they handle personal data and the accessibility of the policy to their customers and the general public. Seventeen firms (55%) were rated *very good* on this indicator, while six entities (19%) were rated *satisfactory* (which meant that they have a policy but it is in process or not easily accessible). Eight entities (26%) were rated *poor* because they do not have a privacy policy in place.

Transparency is not only an indicator of privacy accountability but a key requirement for fair processing in its own right. Based on the proportion of entities that do not have a policy which is easily accessible or at all, there is a large room for improvement in this regard.

International comparison: the results observed in ADGM on indicator 3 differed from the international findings in respect of the proportion of entities which do not have a privacy policy in place being 26% of entities in ADGM compared to 9% of entities in the international results.

Indicator 4 – Responsiveness & Incident Management

Eighteen entities (58%) were rated *very good* in relation to maintaining a documented incident response procedure. Seven entities (23%) were rated *satisfactory*, meaning that they are in the process of implementing incident response procedures, while six entities (19%) were rated *poor* for indicating that they do not have incident response procedures.

In respect of data breaches, fifteen entities (48%) were rated *very good* due to indicating that they have a procedure in place to notify affected individuals in the event of a breach. Nine entities (29%) indicated that such procedures are in process and seven entities (23%) noted that they do not have breach handling procedures.

For incident logs, twenty entities (65%) were rated *very good* for responding that they maintain incident logs in various ways including via compliance tools, breach management programs or registers. Five entities (16%) were rated *satisfactory* for responding that they are in the process of implementing incident logs, and six entities (19%) were rated *poor* for indicating that they do not have any incident log in place.

Twenty entities (65%) were rated *very good* on having policies and procedures in place to respond to requests and complaints from individuals and regulators. Five entities (16%) were rated *satisfactory* for responding that they have procedures in process or under review, while six entities (19%) were rated *poor* for not having any procedures in place.

Overall the majority of entities generally performed well on indicator 4. However, the number of entities in ADGM without data breach handling procedures needs improvement.

International comparison: in respect of indicator 4, entities in ADGM were rated slightly lower on implementation of data breach procedures compared to the international findings. However, entities in ADGM rated higher than the international findings in respect of preparedness to handle requests and complaints.

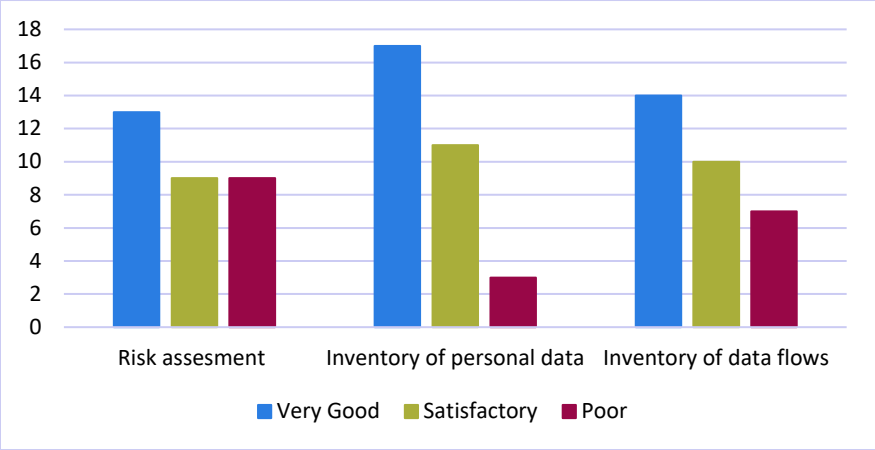
Indicator 5 – Risk Assessment, Documentation and Data Flows

Entities were asked whether they have documented processes to assess risks associated with new products, services, technologies and business models (e.g. data protection impact assessments – DPIAs). Note: DPIAs are not a requirement under ADGM's data protection regime.

Thirteen entities (42%) were rated *very good* for confirming that they do have such processes in place. Nine entities (29%) each indicated that they have processes either under development or not at all.

Seventeen entities (55%) were rated *very good* for indicating that they maintain an inventory of personal data holdings. Eleven entities (35%) were rated *satisfactory* for being in the process of establishing an inventory, and three entities (10%) were rated *poor* for not having an inventory.

Fourteen entities (45%) were rated *very good* for indicating that they maintain records of data flows. Ten entities (32%) were rated *satisfactory* for demonstrating an understanding on data flow record keeping and having records under development, while seven entities (23%) were rated *poor* for not maintaining any record of data flows.



International comparison: ADGM's results on indicator 5 were very similar to the international findings with 55% of entities in the ADGM review maintaining inventories of personal data holdings, as compared to 53% of entities in the international findings.

Best and Worst Results

The three elements that had the most entities in the review receive a 'very good' rating were:

- **Senior level privacy responsibility (indicator 1);**
- **Incident log (indicator 4); and**
- **Responsiveness to complaints (indicator 4).**

The three elements with the most entities in the review receiving a 'poor' rating were:

- **Monitoring data protection performance (indicator 2);**
- **Transparency on handling of personal data (indicator 3); and**
- **Risk assessments (indicator 5).**

Good Practices

Table 1, below, highlights examples of privacy accountability good practice identified by the Office of Data Protection based on the information provided by entities in the review.

Table 1 – Good practice examples

1. Establishing an internal privacy working group, led by a senior individual, to deal with various ongoing privacy matters, such assessment of data handling and staff training plans.
2. Online privacy training systems and sanctions for staff who do not complete the training.
3. Internal privacy resources site with data protection policies, forms, templates and materials.
4. Conducting annual data protection self-assessments and information security audits.
5. Having data protection 'champions' within each office or business unit, in additional to a central senior individual responsible for data protection overall.
6. Mandatory information security and data breach training, specifically.
7. Completing a DPIA before appointing any new data processor.

Chapter 4 – Conclusions and Next Steps

Conclusions

This privacy review, conducted as part of the GPEN Privacy Sweep 2018, is one of many efforts that the Office of Data Protection is carrying out to promote data protection and to better understand the strengths and weaknesses of entities in ADGM, in order to take measures to improve data protection compliance and privacy rights in the ADGM.

The results have demonstrated that the majority of ADGM entities in the review have internal privacy policies in place or in process and a person responsible for data protection.

The results have demonstrated that the majority of entities in the review have internal privacy policies in place or in process and a person responsible for data protection. However, improvement is needed on implementing and/or making accessible privacy policies to customers and the public. The areas of staff training and data breach handling also require attention.

In addition, the review re-affirmed that generally larger and more well-resourced entities are better prepared and that smaller and independent enterprises require support and assistance to ensure compliance with privacy principles and data protection requirements.

What does ADGM want to achieve?

The Office of Data Protection wants to enhance awareness of data protection and compliance by understanding how well entities have implemented privacy accountability into their internal privacy programs and policies.

By conducting this review, the Office of Data Protection gained insights as to where ADGM licensed persons are performing well, as well as where there are weaknesses, in relation to privacy accountability.

Based on these insights, the Office of Data Protection will be able to take measures, such as education and outreach, in order to improve data protection compliance among ADGM licensed persons.

What happens next?

Among other initiatives, the Office of Data Protection will focus its education and outreach efforts specifically on the need for entities in ADGM to focus on training, privacy policies and data breach handling procedures, particularly those that are smaller and independent entities.

Annex A – Review Questionnaire

Statement	Self-Assessment			Evidence
	Achieved	**Partially Achieved**	**Not Achieved**	Please describe how each area has been achieved in practice, and provide evidence where possible
Your organisation has an internal data privacy policy (consistent with legal requirements), which has been embedded into everyday practices				
Your organisation has allocated someone at a sufficiently senior level to be responsible for privacy governance and management				
Your organisation ensures staff are given training regarding the protection of personal information, and you inform them of organisational privacy policies, procedures and best practices				
Your organisations performance is monitored in relation to data protection standards (i.e. by conducting self-assessments and/or audits of your privacy programme and in relation to complaints / enquiries / breaches)				
Your organisation actively maintains policies to explain how you handle personal data, and these easily accessible to customers and the general public				
Your organisation maintains a documented incident response procedure				
In the event of a breach, your organisation has a procedure in place to notify affected individuals and report the breach to the regulator where necessary				
Your organisation maintains an incident log detailing all breaches that occur				
Your organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator)				

Statement	Self-Assessment			Evidence
	Achieved	**Partially Achieved**	**Not Achieved**	Please describe how each area has been achieved in practice, and provide evidence where possible
Your organisation has documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, you conduct privacy impact assessments)				
Your organisation maintains an inventory of your personal data holdings				
Your organisation maintains an inventory of any data flows (for example, data transfers to third parties)				

Disclaimer

This report sets out information and findings in relation to a data protection thematic review conducted by the ADGM Office of Data Protection only. The information provided is not guidance on the operation of ADGM's data protection legislation. This report should be read together with the relevant legislation, in particular, ADGM Data Protection Regulations 2015, as amended, and any other relevant regulations and enabling rules, which may change over time without notice. Information in this report 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 report is strictly at your own risk and ADGM Registration Authority will not be liable for any losses and damages in connection with the use of or reliance on information provided in this report. The ADGM Registration Authority makes no representations as to the accuracy, completeness, correctness or suitability of any information provided in this report.

For more information, please contact the Office of Data Protection by email: data.protection@adgm.com

Published: March 2019