ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

REGISTRATION AUTHORITY
سلطة التسجيل

Office of Data Protection

Data Protection Guide

March 2019
V.02: 27-Mar-2019

1. Contents

2. Introduction 3
3. Overview 4
4. What is Data Protection? 4
5. What is ADGM's Data Protection Regime? 4
6. The Role and Responsibilities of the Data Controller 4
7. Five Key Principles of Data Protection: 5
8. Requirements for Legitimate Processing of Personal Data 7
9. Requirements for Processing Sensitive Personal Data 8
10. Notifications to the Registration Authority 8
11. Transfers of Personal Data out of the ADGM: 9
12. Adequate level of protection 10
13. Transfers out of the ADGM in the absence of an adequate level of protection 11
14. The use of consent for the purpose of data protection 11
15. Difference between Personal Data and Sensitive Personal Data 13
16. Glossary of Defined Terms 14
Disclaimer 15

2. Introduction

Abu Dhabi Global Market

2.1 Abu Dhabi Global Market (ADGM) is a broad based international financial center, 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.

2.2 This guidance ("Guide") is issued under section 28 of the Commercial Licensing Regulations 2015. The Guide has been prepared by the Registration Authority to assist ADGM registered entities in relation to data protection requirements.

Registration Authority

2.3 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, among other things the registration and commercial licensing of businesses operating in or from Al Maryah Island, Abu Dhabi.

The Office of Data Protection

2.4 The ADGM Office of Data Protection is the data protection supervisor for the ADGM. 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 rights of individuals.

The Office of Data Protection also provides guidance to registered entities and receives complaints from individuals.

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

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

3. Overview

3.1 This Guide has been written to assist ADGM registered entities in relation to ADGM's data protection regime. This Guide covers:

- What is data protection;
- The five key principles of ADGM's data protection regime;
- The rights of the Data Subject in relation to their personal data;
- The role and obligations of Data Controller and Data Processor;
- The process of transferring personal data and sensitive data outside ADGM;
- The obligations to notify the Registration Authority;
- The use of consent for the purpose of data protection; and
- Glossary of defined terms.

4. What is Data Protection?

4.1 Data Protection is the process of safeguarding an individuals' personal information, including how personal information is accessed, stored, disseminated and destroyed.

4.2 Data protection regimes exist to create a balance between the rights of individuals to privacy and the needs of organizations to utilize data for the purposes of conducting their business, including sharing personal data with third parties.

5. What is ADGM's Data Protection Regime?

5.1 ADGM's data protection regime consists of the ADGM Data Protection Regulations 2015 (the "Data Protection Regulations").

5.2 The Data Protection Regulations were enacted on October 4, 2015 by the Board of Directors of the ADGM, in exercise of its powers under Article 6(1) of Law No. 4 of 2013 concerning the ADGM (issued by His Highness the Ruler of the Emirate of Abu Dhabi). The Data Protection Regulations make provision for the protection of personal data within the ADGM and for connected purposes. The Data Protection Regulations was amended in 2018 to include updates on matters such as defined terms, data breach notification timeframes and deadlines for notifications to the Registrar, alongside expanded enforcement provisions.

5.3 The Data Protection Regulations control how personal information is used by organisations and businesses registered in ADGM. All entities registered in ADGM that hold or process personal data and must follow the obligations under the Data Protection Regulations to protect such data.

6. The Role and Responsibilities of the Data Controller

6.1 The Data Controller determines the purposes for which, and the manner in which, any personal data are processed and must ensure that any processing of personal data for which they are responsible complies with the Data Protection Regulations. Failure to do so risks enforcement action and compensation claims from individuals.

7. Five Key Principles of Data Protection[1]:

7.1 Data Controllers must ensure that Personal Data which they process are:

a) processed fairly, lawfully and securely;

b) processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights;

c) adequate, relevant and not excessive in relation to the purposes for which they are collected or further Processed;

d) accurate and, where necessary, kept up to date; and

e) kept in a form, which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data were collected or for which they are further Processed.

7.2 Further information on each principle is set out below.

Principle 1. Processed fairly, lawfully and securely

7.3 The Data Protection Regulations requires the Data Controller to process personal data fairly, lawfully and securely. The main purpose of this requirement is to protect the interests of the Data Subjects whose personal data is being processed.

7.4 This principle applies to all actions that a Data Controller undertakes with personal data. In practice, it means:

a) to have legitimate grounds for collecting and using the personal data;

b) do not use the data in ways that have unjustified adverse effects on the individuals concerned;

c) to be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

d) to handle people's personal data only in ways they would reasonably expect; and

e) to make sure they do not commit any unlawful actions with the data.

[1] Section 1.1 Data Protection Regulations 2015

Principle 2. Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights

7.5 The Data Controller must be open about their reasons for obtaining personal data, and that what they undertake with the information is in line with the reasonable expectations of the individuals concerned. In practice, the Data Controller must:

a) be clear from the outset about why they are collecting personal data and what they intend to do with it;

b) comply with the Data Protection Regulation's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data; and

c) ensure that if they wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Principle 3. Adequate, relevant and not excessive in relation to the purposes for which they are collected or further Processed

7.6 The Data Controller must only collect the personal data that they need for the purposes that have been specified. They are also required to ensure that the personal data they collect is sufficient for the purpose for which it was collected. In practice, it means that the Data Controller should ensure that:

a) they hold personal data about an individual that is sufficient for the purpose they are holding it for in relation to that individual; and

b) they do not hold more information than they need for that purpose.

Principle 4. Accurate and, where necessary, kept up to date

7.7 To comply with this requirement, the Data Controller should:

a) take reasonable steps to ensure the accuracy of any personal data they obtain;

b) ensure that the source of any personal data is clear;

c) carefully consider any challenges to the accuracy of information; and

d) consider whether it is necessary to update the information.

Principle 5. Kept in a form, which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data were collected or for which they are further Processed

7.8 The Data Controller is required to retain personal data no longer than is necessary for the purpose that they obtained it for. They must ensure that personal data is disposed of when no longer needed to reduce the risk that it will become inaccurate, out of date or irrelevant. In practice, it means that Data Controllers will need to:

a) review the length of time that personal data is kept;

b) consider the purpose or purposes they should hold the information for in deciding whether (and for how long) to retain it;

c) securely delete information that is no longer needed for this purpose or these purposes; and

d) update, archive or securely delete information if it goes out of date.

8. Requirements for Legitimate Processing of Personal Data[2]

8.1 The conditions for processing personal data are set out in the Data Protection Regulations. At least one of the following conditions must be met whenever the Data Controller processes personal data:

a) The Data Subject has given his written consent to the Processing of that Personal Data;

b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

c) Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;

d) Processing is necessary in order to protect the vital interests of the Data Subject;

e) Processing is necessary for the performance of a task carried out in the interests of the ADGM or in the exercise of the Board's, the Court's, the Registrar's or the Regulator's functions or powers vested in the Data Controller or in a Third Party to whom the Personal Data are disclosed; or

f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the Third Party to whom the Personal Data are disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation.

[2] Section 1.2 Data Protection Regulations 2015

9. Requirements for Processing Sensitive Personal Data[3]

9.1 Due to the nature of sensitive personal data and its vulnerability to be misused, Section 3 of the Data Protection Regulations prohibits the processing of sensitive personal data unless certain criteria are satisfied, including but not limited to:

a) Additional written consent to the processing of this kind of personal data has been obtained from the Data Subject;

b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller; or

c) Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his/her consent.

9.2 Please refer to the Data Protection Regulations for the full list of criteria.

10. Notifications to the Registration Authority[4]

Initial Registration as a Data Controller

10.1 The registration of any data controller residing within Al Maryah Island is mandatory with the Registration Authority. If you are an entity applying to be registered / incorporated in ADGM and will be processing personal data, it is therefore essential for you to complete the Data Protection initial registration form and pay the applicable fee. A Data Controller shall establish and maintain records of any Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.

Application for renewal of Registration as a Data Controller

10.2 Registration as a Data Controller is valid for one (1) year and can be renewed annually by submitting an "Application for renewal of registration – Data Protection" via the Registration Authority's Online Solution available at https://www.registration.adgm.com and by paying the applicable fee. Renewal must be done on every anniversary of the company's incorporation/registration.

Appointment and Cessation of Data Processor

10.3 A Data Controller must notify the Registration Authority of the appointment or cessation of a Data Processor. This notification can done by completing a Notice of Appointment / Cessation of Data Processor through the Registration Authority's Online Solution.

Change in Particulars of Data Processor

10.4 A Data Controller must give notice to the Registration Authority of any change in the particulars of Data Processor. Such notice can be done by completing a Notice of Change of Particulars of Data Processor through the Registration Authority's Online Solution.

[3] Section 1.3 Data Protection Regulations 2015
[4] Section 3.12 Data Protection Regulations 2015

Change in business contact details

10.5 A Data Controller must notify the Registration Authority in case of any change in its business contact details, for example the data protection contact person's name, contact number, email, etc.

Data Breach Notifications within 72 hours

10.6 10.6 An unauthorized intrusion involving personal data is serious issue. Organizations must react appropriately when they become aware of breaches involving customer or employee personal information. A Data Controller must notify the Registration Authority in case of any security breach involving personal data as soon as possible.

10.7 Breach notifications must be filed electronically via the Registration Authority's Online Solution available at https://www.registration.adgm.com.

11. Transfers of Personal Data out of the ADGM[5]:

11.1 Personal data shall not be transferred to a country or territory outside ADGM unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

11.2 The adequacy of the level of protection ensured by laws to which the Recipient is subject, shall be assessed in the light of all the circumstances surrounding a Personal Data transfer operation or set of Personal Data transfer operations, including, but not limited to:

a) the nature of the Personal Data;

b) the purpose and duration of the proposed Processing operation or operations;

c) if the data do not emanate from the ADGM, the country of origin and country of final destination of the Personal Data; and

d) any relevant laws to which the Recipient is subject, including professional rules and security measures.

[5] Section 1.4 Data Protection Regulations 2015

12. Adequate level of protection[6]

12.1 The following jurisdictions have been designated by the Registration Authority as providing an adequate level of protection. This list may be updated from time to time by a publication to such effect on the Registrar's website.

Argentina	Austria
Belgium	Bulgaria
Canada (provided the recipient is subject to the Canadian Personal Information Protection and Electronic Documents Act [PIPED Act])	Cyprus
Czech Republic	Denmark
Dubai International Financial Centre (DIFC)	Estonia
Finland	France
Germany	Greece
Guernsey	Hungary
Jersey	Iceland
Ireland	Isle of Man
Italy	Latvia
Liechtenstein	Lithuania
Luxembourg	Malta
Netherlands	New Zealand
Norway	Poland
Portugal	Romania
Slovakia	Slovenia
Spain	Sweden

[6] Schedule 3 Data Protection Regulations 2015

Switzerland	United Kingdom
Uruguay	United States of America (subject to compliance with the terms of the EU-US Privacy Shield)

13. Transfers out of the ADGM in the absence of an adequate level of protection[7]

13.1 If an ADGM registered entity intends to transfer personal data to a recipient located in a jurisdiction other than in the table above, the transfer is only possible under certain conditions, including but not limited to:

a) the Registration Authority has granted a permit for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of such Personal Data;

b) the Data Subject has given his written consent to the proposed transfer;

c) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;

d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a Third Party;

e) the transfer is made to a person established outside the ADGM who would be a Data Controller (if established in the ADGM) or who is a Data Processor, if, prior to the transfer, a legally binding agreement in the form set out respectively, to these Regulations has been entered into between the transferor and Recipient; or

f) the transfer is made between one or more members of a Group of Companies in accordance with a global data protection compliance policy of that Group, under which all the members of such Group that are or will be transferring or receiving the Personal Data are bound to comply with all the provisions of these Regulations containing restrictions on the use of Personal Data and Sensitive Personal Data in the same way as if they would be if established in the ADGM.

14. The use of consent for the purpose of data protection

14.1 This section highlights key issues that data controllers should be aware of and consider when using the data subject's consent as legal grounds for the processing of personal data. For further information about the use of consent in the area of data protection, please contact the ODP.

[7] Section 5 Data Protection Regulations 2015

Relying on consent for data protection compliance

14.2 Consent of the data subject is only one of several legal grounds that make the processing of personal data lawful. Although many data controllers view consent as the simplest route to compliance with their data protection obligations, it may not always be sufficient on its own. Having consent only ensures compliance with the requirement to process data fairly and lawfully. Data controllers must still comply with the remaining data protection principles. This means that the data controllers will not be permitted to process personal data that are inaccurate or out of date, unnecessary, irrelevant or excessive for the specific purposes for which they were collected, even if the data subject had previously consented.

14.3 Additionally, data controllers may only rely on consent as grounds for lawful processing of personal data if the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment.

Definition of consent

14.4 To be valid in a data protection context, consent must be freely given, specific, informed, and unambiguous. The data subject must also signify his agreement to the processing of his personal data.

- Consent will only be deemed freely given if it is voluntary and if data subject is able to exercise a real choice, i.e. there is no risk of deception or coercion.

- Consent will only be deemed specific if it is given with respect to the type of personal data that is processed, and the exact purpose for which it is processed.

- Consent will only be deemed an informed consent if the data subject was given accurate and full information of all relevant issues in a clear and understandable manner. This should include the nature of the data processed, the purpose of the processing, the recipients of possible transfer, the right of the data subject, etc.

- Consent will only be deemed unambiguous if the procedure to seek and to give consent leaves no doubt that the data subject does in fact agree to that processing. Methods to obtain unambiguous consent include express statements by the data subject, online forms that include a visible tick box to be ticked by individuals who agree to their data being processed in a particular way that is explained on the online form or a documents to which that form links, express oral consent, etc.

Express or Explicit consent

14.5 Express or explicit consent encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use of disclosure of their personal information and they respond actively to the question orally or in writing, consent which is inferred or implied will not normally meet the requirement of explicit consent.

At what stage must consent be obtained?

14.6 As a general rule, the data controller must obtain consent before processing personal data, particularly if it is a pre-condition for lawful processing.

What happens When a Data subject withdraws his consent?

14.7 The data subject's withdrawal of consent has no retroactive effect, this means that it will not make previous data processing that was based on the original consent unlawful. However, a withdrawal should, in principle, prevent any future processing of the data subject's data unless the processing can be justified by other legal grounds.

15. Difference between Personal Data and Sensitive Personal Data

15.1 The difference between personal data and sensitive personal data may in certain instances be difficult to define. For example, names and surnames in connection with addresses and dates of birth are personal data rather than sensitive personal data. However, more sensitive details such as ethnicity or religion may be inferred from these details, as frequently particular surnames are associated with a certain religion or ethnicity, or possibly both.

15.2 This does not necessarily mean that in order to maintain these names on client databases you would have to comply with the requirements for processing sensitive personal data. But where the data processor is processing such names due to the specific reason that they indicate a certain religion or ethnicity, e.g. to send advertising or marketing materials for items or services that are targeted specifically at persons of this particular religion or ethnicity, then this would constitute the processing of sensitive personal data.

15.3 In all instances assumptions about data subjects should be made with caution as such assumptions may lead to the collection of inaccurate personal data.

16. Glossary of Defined Terms[8]

Term	Meaning
Data:	any information which– (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; or (c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System.
Personal Data:	Any information relating to an identified natural person or identifiable natural person.
Identifiable Natural Person:	A natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Data Controller:	Any person in the Abu Dhabi Global Market (excluding a natural person acting in his capacity as a staff member) who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Processor:	Any person (excluding a natural person acting in his capacity as a staff member) who Processes Personal Data on behalf of a Data Controller.
Data subject:	The natural person to whom Personal Data relate.
Processing:	Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and "Processed", "Processes" and "Process" shall be construed accordingly.
Recipient:	Any person to whom Personal Data are disclosed, whether a Third Party or not, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
Sensitive Personal Data:	Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life.

[8] Section 7.20 Data Protection Regulations 2015

Disclaimer

This Guide provides information on completing the annual Data Protection Register Renewal obligation. This is only a guide and should be read together with the relevant legislation, in particular, ADGM Companies Regulations 2015, ADGM Data Protection Regulations 2015 and any other relevant regulations and enabling rules. The Guide only refers to the procedures that need to be completed in relation to the Registrar. It does not cover other requirements such as obtaining relevant permits from third parties, if necessary. Further advice from a specialist professional may be required.

For more information, please contact the Office of Data Protection by:

Telephone: +971 2 333 8888

Email: Data.Protection@adgm.com

In person: 3rd floor, ADGM Building, Abu Dhabi Global Market Square, Al Maryah Island, Abu Dhabi, United Arab Emirates.

Published: March 2019