CHECKLIST: ABU DHABI GLOBAL MARKETS DATA PROTECTION REGULATIONS 2015

1. INTRODUCTION

- The Data Protection Regulations, 2015 ("**DPR**") were enacted on 4th October, 2015. The DPR governs the processing of any personal or sensitive personal information/data by organisations registered in the Abu Dhabi Global Market ("**ADGM**").

  The DPR entrusts the ADGM Registration Authority[1] ("**Registrar**") with enforcing and ensuring compliance with the DPR and also the Office of Data Protection ("**ODP**"). The ODP is responsible for promoting data protection within ADGM, maintaining the register of data controllers, enforcing the obligations upon Data Controllers and upholding the rights of individuals. It provides a range of information, guidance (in the form of DPR Guides) and tools not only to entities operating within ADGM, but also to individuals and the general public.

- All organisations registered in ADGM should demonstrate compliance with the DPR. The DPR proposes significant penalties (up to USD 15000/-) for non-compliance with the DPR and as a result of which directions were issued against such party by the Registrar.

- This checklist is intended to be a starting point for organisations to understand their obligations under the ADGM laws. The checklist lists out compliance requirements and action items for organisations under five heads: (i) understanding the scope for the DPR; (ii) accountability; (iii) fair and lawful processing; (iv) data subjects' rights; and (v) transferring data outside ADGM. The checklist indicates whether a set of actions is relevant for data controllers ("**DCs**") or data processors ("**DPs**") and obligations under the DPR for entities outside the ADGM ("**Non-ADGM entities**") who are recipient of data from ADGM regulated entities, or all three. It also identifies the relevant teams that need to be involved in each set of actions:

Legal and Compliance	🔴
Technical and IT	🔵
Customer Relations	🟢

[1] The ADGM Registration Bureau located at Abu Dhabi Global Market Square and as established under Article 11 of the Law No. 4 of 2013 (concerning Abu Dhabi Global Market), *available at* https://www.adgm.com/-/media/project/adgm/legal-framework/documents/abu-dhabi-legislation/abu_dhabi_law_no_4_of_2013.pdf.

Public Relations

HR

2. COMPLIANCE CHECKLIST

(I) UNDERSTANDING SCOPE AND PREPARING FOR THE LAW

Subject	Description of DPR requirement	Action	Relevant DPR provision
Scope (DC/DP)	The DPR applies to the processing of 'personal data' by all entities registered in ADGM. Processing includes, but is not limited to the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, or any other activity related to data. "Personal data" in this context refers to information relating to an identified natural person or identifiable natural person (identifiable natural person has further been defined as a natural person who can be identified, directly or indirectly, by reference to one or more factors specific to his physical, physiological, mental, economic, social or cultural identity).	Organisations should: ▪ Identify if they process any personal data (i.e. data that relates to a natural person or identifiable natural person). ▪ Understand if they determine the purpose and means of data processing. If so, they will be DCs. ▪ Understand if they are only processing data on behalf of another entity. In that case, they may be DPs. ▪ Identify if their data processing activities are exempted under the DPR.	Section 21

	The DPR regulates data-processing activities of DCs and DPs.		
Territorial scope (DC/DP)	The DPR applies in the ADGM to personal data processing by organisations and businesses registered in the ADGM and also recipients of personal data by Non-ADGM entities from ADGM entities. The Board[2] (as specified under section 16 of the DPR) can make rules to exempt DCs from their obligations under the DPR. *The grounds on which the Board may exempt DPR application to an entity have not been outlined in the DPR.*	Organisations should: ▪ Identify if they are registered in the ADGM and whether they process personal data; ▪ Identify whether they are a DC, and if so whether they are eligible for an exemption from the DPR compliances as mandated by the Board, which may be issued on a case-by-case basis given these have not specifically been outlined in the DPR.	Sections 21 and 19

(II) ACCOUNTABILITY

Accountability: Governance and Systems

Subject	Description of DPR requirement	Action	Relevant DPR provision
Security safeguards (DC/ DP)	DCs should adopt appropriate security and organizational safeguards, after considering the nature and purpose of processing, risks associated with the processing, nature of the personal data	Organisations should: ▪ Determine the nature and types of data being processed and the risks associated with processing information of that type.	Section 9

[2] As established under Article 4 of the Law No. 4 of 2013 (Concerning Abu Dhabi Global Market), *available at* https://www.adgm.com/-/media/project/adgm/legal-framework/documents/abu-dhabi-legislation/abu_dhabi_law_no_4_of_2013.pdf.

	being protected, and likelihood and severity of harm that could arise from such processing. These measures should protect personal data against the risk of unauthorised or unlawful intrusion, against unauthorized or unlawful processing and against accidental loss or destruction or damage to such personal data (including any loss of devices carrying such personal data), whether physical or electronic. DPs are required to provide sufficient guarantee in respect of technical security measures being adopted and organizational measures governing the processing to be carried out, when they process personal data on behalf of the DCs. *However, the DPR does not lay down any specific security measures that need to be mandatorily adopted by the DCs/DPs.*	▪ Develop procedures to assess such risks associated with processing and the likelihood and severity of harm to individuals from their data-processing activities. ▪ Develop procedures to mitigate those risks using appropriate security safeguards. ▪ Include appropriate techniques such as de-identification, encryption, identity and access management, data loss prevention, data retrieval mechanisms as required. ▪ Undertake review of security safeguards periodically and maintain a record of the review. ▪ Ensure third party contractors have appropriate security controls.	
Breach notification (DC)	DCs should notify the Registrar of any data breach such as an unauthorised intrusion (whether physical, electronic or otherwise) or loss of any devices containing personal data. The DC is required to notify the Registrar as soon as possible (within 72 hours). The DP is required to promptly notify the DC of a data breach.	Organisations should: ▪ Develop data breach response procedures to notify the Registrar as soon as possible in case of a breach. ▪ Put in place procedures to assess situations that may lead to a data breach. ▪ Build processes to identify a data breach and notify the Registrar of such a breach as soon as possible. ▪ Prepare templates for notifying the Registrar case of a data breach[3].	Section 9(5) of the DPR and Schedule 2 (DC to DP transfers) Clause 5 (d)(ii)

[3] A data breach can be reported by following the process given here.

	It is unclear whether the data breach notification to the Registrar is to be made within 72 hours of the occurrence of the security incident or the DC becoming aware of the occurrence of the security incident.	▪ Review contracts with third parties and DPs to ensure that DC will be able to notify the Registrar in time. ▪ Review liability provisions in third party contracts for breaches caused by third parties. ▪ Maintain and review insurance coverage for data breaches.	

Accountability: Compliance with the Registrar's Directions or Orders

Subject	**Description of DPR requirement**	**Action**	**Relevant DPR provision**
Compliance with Registrar's Directions (DC/DP)	The Registrar has the power to access all personal data processed by any DC or DP; collect any information that is necessary for the performance of the Registrar's supervisory duties; prescribe formats for compliance with the DPR and make recommendations or issue warnings/directions to DCs. The Registrar can also require specified information in relation to the processing of personal data or otherwise. *However, the Registrar's power to access any 'specific information' from a DC is vague. Since what constitutes 'specific information' is not clear, it may be the case that the Registrar has the power to gain access to any information/data collected by the DC.*	Organisations should: ▪ Comply with any request or direction made by the Registrar. ▪ Develop processes to respond to the Registrar's directions or requests. ▪ Keep a record of the kind of data collected and processed and the purpose for which such data was processed by DPs. ▪ DCs should keep a record of the DPs or any third parties with whom any data has been shared.	Section 14

(III) FAIR AND LAWFUL PROCESSING

Subject	Description of DPR requirement	Action	Relevant DPR provision
Basis for processing personal data (DC)	Any processing should be conducted under one of the legal basis/grounds specified. These include an written consent of the data subject, performance of a contract to which data subject is party, protecting the vital interests of a data subject, state action, compliance of a legal obligation by DC, compliance with court order, emergencies, necessity in the interest of the ADGM, performance of the ADGM authorities' (court, Board, Registrar, or the regulator) functions, necessity for pursuance any legitimate interests by the DC or any third party with whom the personal data is shared. The DPR prohibits processing of sensitive personal data except in limited circumstances, which include but are not limited to the following, obtaining the data subject's additional written consent, and the processing is necessary for performing any obligations by the DC or protecting the vital interests of the data subject or compliance with DC's legal obligations or to uphold the legitimate interests of the DC. Please note that	Organisations should: ▪ Identify and document a legal basis for processing personal data or sensitive personal data, which must align to those outlined in the DPR for processing these categories of data. ▪ Identify whether the organisations process any kind of sensitive personal data, sensitive personal data has been defined under the DPR as personal data that reveals (directly or indirectly) an individual's race, ethnicity, political or religious beliefs, trade union membership, health or sexual information. ▪ Identify the reasons for processing of any sensitive personal data or personal data and the manner of obtaining written and explicit consent for processing such data. ▪ Before relying on consent, understand if any of the other basis are applicable. For instance, if personal data has to be shared under a law or for compliance with court order, separate consent would not be required. ▪ Explain the basis of processing in their privacy policies/ notices.	Section 2

	there are certain exceptions built in when the interests of the data subject are more compelling than that of the DC's, then the DC's interests will be overridden by the protection required for the compelling interests of the data subject and the sensitive personal data may not be processed. However, it is also to be noted that the DC may not need to satisfy all these requirements for processing sensitive personal data if it has already obtained a permit from the Registrar which allows it to process the sensitive personal data and in a case where the DC applies adequate safeguards with respect to processing personal data. The DPR guides further states that in processing the data certain principles should be followed which are as set out below: • The processing should be done on legitimate grounds; • The data should not be used in ways which may have unjustified affects on the individual concerned; • The DC needs to be transparent about the intended use of the data and give the data subjects appropriate privacy notices when collecting the personal data;		

	• The DC is expected to handle data only in ways reasonably expected by the data subject; • DC must not commit any unlawful actions while processing or using the data. *The meaning of 'legitimate interests' of the DC is unclear. This term may be interpreted along the lines defined under the General Data Protection Regulations, 2018 ("**GDPR**") of the EU.*		
Consent (DC)	In order to lawfully process personal data, DCs must comply with strict consent requirements. They should obtain written consent that is free, specific, informed and unambiguous. In case of sensitive personal data, the DCs will be required to obtain additional written consent, in addition to the written consent obtained for processing of personal data. Any kind of consent that is either inferred or implied will not suffice as additional consent. In case the data subject withdrew his consent, such withdrawal has no retroactive effect, which means this will not make the previous data processing based on original consent unlawful. However, a withdrawal, should effectively prohibit the DC	Organisations should: ▪ Ensure that consent is sought before processing. ▪ Determine how to gain written consent for processing of personal data and additional written consent for the processing of sensitive personal data. ▪ Maintain clear records of written consents obtained from data subjects to be able to demonstrate that the data subject had provided free, specific, informed and unambiguous consents at the time of processing. ▪ Ensure that provision of goods or services or performance of a contract is not conditional on consent to processing any personal data that is not necessary for that purpose. ▪ Ensure that consent is free, specific and clear. ▪ Review existing consents to ensure compliance with the new requirements and where non-compliant, draft new consent forms to seek fresh consent. ▪ Create mechanisms to allow data subjects to withdraw consent.	Sections 2 and 3 read with Data Protection Guide

	from processing the data subject's data unless the processing can be justified by other legal grounds.		
Privacy notice  (DC)	If the personal data is obtained directly from the data subject, the DCs should notify data subjects as soon as possible (upon commencing the data collection) about the identity of data controllers and the purpose for which the processing of the data is intended (collectively, "**Mandatory Information**"). The DC may additionally inform the data subject of the following (if it is necessary given the circumstances): recipients or categories of recipients of the personal data, whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the personal data concerning him, whether the personal data will be used for direct marketing purposes and whether the personal data will be processed on the basis of section 3 (1)(g) i.e. necessary for upholding the legitimate interest of the DC in the international financial markets. Further, if the DC is not directly processing the personal data from the data subject or if the DC is making any disclosures to a third party of such	Organisations should: ▪ Review and update privacy notices to make them DPR-compliant (or develop privacy notices where they do not exist). ▪ Develop processes to provide information in a clear and easily comprehensive form.	Section 6

	data, the DC is obligated to inform the data subject, the manner of collection, whether any questions posed are mandatory, use of personal data for direct marketing, whether the data will be processed to uphold the DC's legitimate interests, and the procedure for exercise of data subject rights (collectively, "**Additional Information**"). The DC does not need to inform the data subject about the recipients of his/her data, if the DC thinks that a data subject already knows about the recipients. If the personal information has not been obtained from the data subject, then the DC must notify the data subject of the Mandatory Information and the Additional Information (if necessary) as soon as the processing begins. The DC need not inform the data subject of the Mandatory and Additional Information if the DC reasonably thinks that the data subject may already know such information or if providing such information is impracticable or requires disproportionate effort.		

(IV) DATA SUBJECTS' RIGHTS

Subject	Description of DPR requirement	Action	Relevant DPR provision

Right to access, rectify, erase, block or object to processing of personal data  (DC)	The data subject has the right to ask the DC (i) whether or not such data subject's personal data is being processed; (ii) if so, for what purpose is the data being processed; (iii) categories of personal data that is being processed; and (iv) the categories of recipients with whom the personal data is shared. The data subject can also request the DC to provide information about their personal data, which is currently being processed, in an intelligible form. The data subject can ask the DC to rectify, block or erase any data which is being processed, provided that such processing does not comply with the DPR. A data subject has the right to object to the processing of his/her personal data at any time on reasonable ground relating to his particular situation. The data subject also has the right to be informed if his/her personal data is used for direct marketing or shared with third party and expressly object to such use or disclosure in this manner of his/her personal data. *However, the DPR does not specify any format or timelines for making such requests. It is not clear whether the DC is bound to comply with such*	Organisations should: ▪ Develop processes to allow individuals to make such requests. ▪ Create templates for summaries of personal data and processing activities to be provided to data subjects, upon request. ▪ Consider automated means to provide confirmation and summary of processing activities to data subjects. ▪ Maintain a list of entities with whom the personal data of is shared. ▪ Develop internal processes that enable correction of inaccurate data, completion of incomplete data, and update old data in a timely manner. ▪ Create a system whereby relevant stakeholders are notified of any change to the data pursuant to such requests. ▪ Assess different machine-readable formats. ▪ Understand the legal mechanisms under which such requests can be resisted. ▪ Develop processes to determine the relevance of the data to the purpose of collection. ▪ Inform other stakeholders that the data subject has requested the erasure of personal data.	Sections 10 and 11

	requests. We opine that the DC is required to comply with such requests. Further, it is unclear as to what comprises 'reasonable grounds' with respect to a data subject's right to object to the processing of his/her personal data.		

(V) TRANSFERRING DATA OUTSIDE ADGM

Subject	Description of DPR requirement	Action	Relevant DPR provision
Cross-border transfers (DC/DP)	DCs may transfer personal data outside ADGM, only if the jurisdiction to which the data is being transferred, contains adequate levels of protection as notified under Schedule 3 (Jurisdictions with Adequate Levels of Protection) of the DPR. "Adequate Protections" in this context refers to protective measures taken by the DC or data exporter which may include but not be limited to the nature of the personal data, the purpose and duration of the proposed processing operation or operations and if the data does not emanate from ADGM, the country of final destination of the personal data, and any relevant laws to which the recipient is subject including professional and security measures.	Organisations should: ▪ Review processes for cross-border data transfers. ▪ Develop specific processes to conduct transfer of sensitive personal data. ▪ Ensure that written consent and additional written consent is obtained before transferring data outside ADGM. ▪ Consider preparing a template for requesting specific approval from the Registrar. ▪ Formulate country-specific processes for cross-border transfers.	Section 5

	Data transfers to jurisdictions without adequate levels of protection are permitted in certain cases, which include, but are not limited to the following: obtaining a permit from the Registrar; gaining the data subject's written consent for the transfer; performance of a contract between DC and DS and/or a third party; as a necessity for any legal compliance by the DC; or transfers between group companies (provided that the recipient company agrees to comply with the DPR).		

This checklist is intended as an overview of key action items for compliance with the DPR. This should not be construed as, or relied upon, as legal or professional advice.

****