ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

CONSULTATION PAPER
NO. 6 OF 2020

NEW DATA PROTECTION REGULATORY FRAMEWORK

19 November 2020

Contents

Introduction

Why are we issuing this paper?

The Abu Dhabi Global Market ("**ADGM**") has issued this Consultation Paper to invite public feedback and comments on proposed new Data Protection regulatory framework for ADGM. The proposal is to implement a new data protection regulatory framework by enacting new, stand-alone regulations to replace the existing regulations. These changes are in light of changes occurring globally, including the introduction of GDPR in the EU.

Who should read this paper?

This paper will be of interest to persons who may be considering setting up business in the ADGM, Data Controllers and Data Processors in ADGM and their respective professional advisors. It will also be of interest to individuals who have provided or intend to provide their personal data to entities operating within ADGM.

How to provide comments

All comments should be in writing and sent to the address or email specified below. If sending your comments by email, please use the Consultation Paper number in the subject line. If relevant, please identify the organisation you represent when providing your comments. ADGM reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise at the time of making any comments. Comments supported by reasoning and evidence will be given more weight by the ADGM.

What happens next?

The deadline for providing comments on this proposal is **Saturday, 19 December 2020**. Once we receive your comments, we will consider whether any modifications are required to the proposed enhancements to the Data Protection regulatory framework. The Board will then proceed to enact the proposed new regulations.

You should not act on this proposal until the new regulations are issued. We will issue a notice on our website when this happens.

Comments to be addressed to:

Consultation Paper No. 6 of 2020
Abu Dhabi Global Market
Abu Dhabi Global Market Square
Al Maryah Island
PO Box 111999
Abu Dhabi, UAE
Email: consultation@adgm.com

Background

1. An increase in personal data used by businesses, and advances in technology, makes strong legislation that protects personal data an important part of a global economy as well as a successful international financial centre. It is recognised internationally that specific dedicated and comprehensive legislation on data protection is a fundamental component in protecting the rights of individuals with respect to their personal data and in order to provide fairness, transparency and accountability. The ADGM was cognizant of this from the very start by enacting a strong data protection framework in 2015.

2. In 2015 ADGM enacted the Data Protection Regulations, with minor amendments in 2018 and 2020 (together, the "**Existing Regulations**"). The Existing Regulations are based on the OECD Privacy Guidelines, the European Data Protection Directive (Directive 95/46/EC on the protection of individuals with regards to the processing of personal data) (the "**Data Protection Directive**") and the UK Data Protection Act ("**DPA**") 1998. Since then both the Data Protection Directive and the UK DPA 1998 have now been superseded by the European Union's Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data (the "**GDPR**") and the UK DPA 2018.

3. The GDPR is a complex and detailed EU regulation designed to protect the fundamental rights of natural persons with respect to their personal data. It has two objectives, namely to enhance data protection rights of individuals, and to improve business opportunities by facilitating the free flow of personal data.

4. Although other jurisdictions have their own approaches to data protection, ADGM believes that the GDPR is the appropriate internationally accepted best practice benchmark, for the following reasons:

   (a) **High-water mark**: The GDPR is generally considered to have set a high-water mark for data protection regulation globally, including by providing strong protections for individuals and imposing significant financial penalties for contraventions. As a result, any regime based on the GDPR is more likely to be compliant with the core principles of other, less demanding regimes.

   (b) **Global alignment**: a number of jurisdictions have either already introduced new data protection laws based on the GDPR or are planning to do so. This includes Brazil (the Brazilian Data Protection Law, Law No. 13,709/2018), Malaysia, which recently announced updates to its Personal Data Protection Act 2018, and California with the enactment in 2018 of the Consumer Privacy Act, which is inspired by the GDPR. Moreover, while voluntary certification initiatives such as the APEC Cross Border Privacy Rules contain similar obligations in respect of accountability and security standards, they do not replace domestic privacy laws and do not reach the standard, or contain the enforcement powers, included in the GDPR. We believe consistency with other international data protection regimes is likely to be attractive to multi-national companies operating within ADGM and ADGM companies seeking international expansion.

   (c) **Proven effectiveness**: The GDPR came into effect in May 2018, and in that time companies and regulators have gained experience of how it works in practice, a significant amount of guidance has been issued, and practitioners are in a position to

evaluate the effectiveness of various aspects of the legislation. This is in addition to the overall acceptance of GDPR in business operations globally as the standard required to be met for data protection.

5. Accordingly, we are inviting comments on the proposal to align the legislative framework in the ADGM with GDPR, as well as the Consultative Committee of the Convention for the protection of individuals with regard to the processing of personal data ("**Convention 108+**") and the UK DPA 2018.

6. We also propose several specific departures from the GDPR, including where:

   (a) it is required in order to be adapted to the needs of ADGM; and

   (b) there is an opportunity to be more proportionate and commercially friendly without undermining the key ambition of achieving a high standard of protection for personal data.

7. The changes under consideration are summarized in this paper and set out in more detail in **Annex A - Data Protections Regulations 2020**.

8. Unless otherwise defined, capitalized terms referred to in this paper have the meanings attributed to such terms as contained in the Existing Regulations and the Interpretations Regulations 2015.

Policy Considerations

A. Approach and structure of updates to the ADGM data protection framework

9. There is a global trend towards enhancements in data protection legislation with many jurisdictions now using the GDPR as a reference point. This trend reflects both a recognition for the importance of rights concerning personal data, as well as a need to stay up to date with global changes as part of a global economy. Accordingly, ADGM proposes to implement its new data protection regulatory framework by enacting new, stand-alone Data Protection Regulations (the "**New Regulations**") to replace the Existing Regulations, with the GDPR as the reference point.

10. The advantages of enacting New Regulations based on the GDPR include:

    (a) enabling global businesses to capitalise on their familiarity with the GDPR and making it easier to adopt a consistent, global approach to data privacy (including group-wide data protection policies and procedures);

    (b) assisting ADGM's supervisory authority to follow practices adopted by EU supervisory authorities and the European Data Protection Board that may be useful in ADGM; and

    (c) providing potentially useful precedent for where there may be disputes before the ADGM Courts, considering such cases in ADGM.

11. ADGM proposes to broadly align the New Regulations with the GDPR, unless there is a compelling reason for divergence. Such alignment would include using similar drafting to avoid interpretation issues. This would include using:

    (a) **key definitions** such as personal data, processing, consent, data controller, data processor and recipient, as these are foundational building blocks of the regime;

(b) **Key data protection principles -** which will require the introduction of standalone principles of accountability and transparency which are not present in the Existing Regulations;

(c) **Lawful bases** for processing - for special category personal data (such as health) this would mean the replacement of some of the broader lawful bases found in the Existing Regulations with more specific additions (from the UK DPA 2018);

(d) **Individual rights** - introduction of new rights for data subjects (i) not to be subject to a decision which is based solely on automated decision making, including profiling, and (ii) data portability (the right to receive personal data in a format which allows data subjects to transmit it to another data controller);

(e) **Security obligations** - which require data controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

(f) the ability of the supervisory authority to **approve industry-specific codes of conduct** and **establish a certification regime** for compliant data controllers and data processors; and

(g) the **trigger point for notification of a data breach** to the supervisory authority and affected individuals. The notification requirements in the Existing Regulations differ from and are, in some respects, more extensive than the GDPR requirements. Aligning with the GDPR would simplify the analysis carried out by businesses in respect of where and when notification is required. This is particularly relevant in the context of a multi-jurisdictional data breach where data controllers are considering multiple laws regarding notification.

Q1: DO YOU HAVE ANY COMMENTS ABOUT THE PROPOSAL TO BROADLY ALIGN THE NEW REGULATIONS WITH THE GDPR?

B. Territorial Scope

12. Since GDPR has an extra-territorial intention (i.e. it is intended to apply to organisations outside of the EU), the question of territorial scope in the New Regulations requires consideration.

13. Given the relative size of ADGM and the limitations imposed by ADGM's legislative powers in Federal Law No. 8 of 2004, it is outside ADGM's powers for the New Regulations to have the extensive a territorial scope as the GDPR. Accordingly, ADGM proposes that the territorial scope of the New Regulations will only cover Personal Data processed in the context of an establishment within ADGM.

14. There is detailed EU guidance to support this approach; broadly it would include where a business is established in ADGM but processes data through an establishment outside ADGM, where that processing is inextricably linked to the business carried on inside ADGM.

15. However, where a data controller is only connected to ADGM because it uses a Data Processor located inside ADGM, the New Regulations would not apply to the data controller (although the Data Processer itself would be captured).

Q2: DO YOU HAVE ANY COMMENTS ABOUT THE PROPOSED SCOPE OF THE NEW REGULATIONS?

C. Data subject rights – response time limits

16. Under the GDPR, rights relating to access, rectification, erasure, restriction of processing, portability, objection and automated decision making have an initial time limit for a response of one month, which can be extended by two months for complex requests. Since the introduction of the GDPR, there has been an increase in individuals seeking to use these rights, which has meant that many businesses find it challenging to comply within the timeframe. In consideration of this challenge, and in order to ensure a person's rights while reducing the burden on businesses, ADGM propose an initial two-month time period for compliance with data subject rights requests, which can be extended by a further two months for complex requests.

17. Further, a failure to respond within the prescribed time period would not necessarily lead to a fine, as the supervisory authority may use its discretion to decide on the most appropriate course of action in the specific circumstances.

Q3: DO YOU HAVE ANY COMMENTS ABOUT THE PROPOSED RESPONSE TIME LIMITS? IN CASE OF ANY CONCERNS, PLEASE EXPLAIN WHY.

D. Accountability and governance

18. ADGM proposes to replicate the core requirements of accountability and governance from the GDPR, with some simplification. This means that the key parts of the accountability and governance framework (as listed below) would be included, but with less detail than in the GDPR. This approach signals the key points regarding accountability and governance to Data Controllers but will also allow the supervisory authority some flexibility to adapt to the needs of organisations in ADGM and provide detailed guidance which can be tailored towards different sectors and updated as technologies evolve.

Data protection by design and by default

19. The concept of "data protection by design and by default" requires Data Controllers to integrate data protection considerations into business practices from the design stage and throughout the lifecycle. The concept is intended to encourage organisations to consider data protection upfront and have default settings as "privacy friendly".

Records of data processing

20. Data Controllers (subject to the SME exception, see further below) would be required to keep records of their data processing activities, including (i) the purposes of processing; (ii) what Personal Data is being held and on what types of individuals; (iii) identifying who the data has been shared with; (iv) whether data has been sent outside of ADGM in respect of each type of processing (and if so, the safeguards in place); (v) retention periods; and (vi) security measures. This is intended to enable businesses to demonstrate how they are complying with the law by providing a clear view of their data processing activities and the associated compliance steps. The supervisory authority should be able to request this record to help gain an overview of a Data Controller's approach to compliance.

Data protection impact assessments

21. Data Protection Impact Assessments ("**DPIAs**") are a way for Data Controllers to consider and document high risk processing activities, and include an assessment of proportionality, identification of risks and outline the safeguards put in place to protect data subjects. DPIAs are only required where processing is considered to pose a high risk to the rights of data subjects. Under the GDPR, in certain high risk processing scenarios, DPIAs must be reviewed by the

supervisory authority, which can impose recommendations or restrictions in respect of the proposed processing activity.

22. The New Regulations include a power for the ADGM supervisory authority to publish a list of processing activities which it considers high risk, and where a DPIA is likely to be required, from time to time.

Data Protection Officers (*DPOs*)

23. The New Regulations proposed make provision for Data Controllers, including each of the ADGM Authorities, to appoint a DPO (subject to the SME exception, see further below). However, to ensure that businesses in ADGM can leverage their global DPO role, the DPO does not need to be present in ADGM or be an employee of the Data Controller. To help reduce compliance costs for Data Controllers, the DPO also can hold multiple roles in a business and/or operate in respect of multiple businesses (including permitting the DPO role to be outsourced to a third party professional services firm), so long as no other role conflicts with that individual's obligations as DPO.

SME exception

24. Despite the importance of the accountability obligations described above, it has been recognised that they can place significant burdens on Data Controllers, particularly small and medium size enterprises ("**SME**"). ADGM proposes to include an exception from (i) record keeping; and (ii) the DPO obligations, for SMEs (defined in the New Regulations as those with fewer than 5 employees in ADGM and which perform processing of Personal Data which is low volume and low risk).

Q4: DO YOU HAVE ANY COMMENTS ON WHAT:

(A) IS REQUIRED BY THE CONCEPT OF 'BY DESIGN AND BY DEFAULT'?
(B) THE DEFINITION OF HIGH RISK PROCESSING IS?
(C) THE REQUIREMENTS ARE FOR RECORD KEEPING?
(D) THE REQUIREMENTS ARE AROUND APPOINTING A DPO FOR NON-SME DATA CONTROLLERS?
(E) IS MEANT BY THE SME EXCEPTION?

E. International transfers

Binding Corporate Rules and model clauses

25. The Existing Regulations include a provision which sets out a method of intragroup transfer based on a "global data protection compliance policy" similar to the EU concept of binding corporate rules ("**EU BCRs**"). ADGM proposes that the intragroup data transfer mechanism is aligned to the EU BCRs, with the supervisory authority given the power to introduce a fast track approval process for EU BCRs.

26. In addition, the New Regulations incorporate the European Commission's most recently updated model clauses by reference to ensure that the updated versions are automatically incorporated into the New Regulations once approved by the supervisory authority. This would allow multi-national businesses to adopt a single form of data transfer agreement for use across multiple jurisdictions, including ADGM.

Derogations from restrictions on international transfers

27. Under the GDPR, there is a general rule that personal data may not be transferred out of the jurisdiction (in that case, the EEA), subject to specific derogations. The same base position is adopted in the New Regulations.

28. ADGM proposes that the derogations to the restriction on transfer should be narrowed, whilst still allowing the regulatory bodies in ADGM to achieve their regulatory objectives and meet international obligations, where:

    (a) the Data Controller has obtained explicit consent from data subjects;

    (b) the transfer is necessary for the performance of a contract between the data subject and the Data Controller;

    (c) the transfer is necessary for the performance of a contract between the Data Controller and another person (for the benefit of the data subject);

    (d) the transfer is necessary for important reasons of public interest in ADGM;

    (e) the transfer is required by law enforcement agencies of the UAE;

    (f) the transfer is necessary for the establishment, exercise or defence of legal claims; and

    (g) the transfer is necessary to protect a person's life.

Q5: DO YOU HAVE COMMENTS ON THE PROPOSED APPROACH WITH BCRS AND MODEL CLAUSES?

Q6: WE INVITE COMMENTS FROM COMPANIES CURRENTLY RELYING ON A DEROGATION IN THE EXISTING REGIME THAT IS NOT PROPOSED IN THE NEW REGULATIONS.

F. Data protection fee

29. Although the GDPR does not require supervisory authorities to levy an annual data protection fee or maintain a register of Data Controllers, it is accepted that EU Member States may use a fee paid by Data Controllers as a way of funding the work of the supervisory authority.

30. ADGM proposes to maintain the flat fee structure of the Existing Regulations, but applying it only to those Data Controllers that are required to engage a DPO (i.e. excluding SMEs).. This approach is considered the most proportionate to the risks posed and resourcing needs of the supervisory authority in supervising and monitoring Data Controllers.

Q7: WE INVITE COMMENTS ON THE PROPOSAL TO EXEMPT SME'S FROM DATA PROTECTION FEES.

G. Independent supervisory authority

31. An important part of a data protection regime is monitoring how the rules are being complied with and ensuring appropriate enforcement in cases of non-compliance. ADGM proposes to maintain its current Office of Data Protection within the Registration Authority but with clear operational independence from the Registrar's other regulatory functions. The Office of Data Protection will be empowered with the following independent features:

    (a) responsibility for monitoring and enforcing the application of the New Regulations, promoting awareness amongst Data Controllers, Data Processors and the general public and handling complaints received from data subjects;

(b) the ability to act with complete independence and impartiality in performing its duties and exercising its powers, free from external influence and neither seeking nor accepting instructions from the Registrar;

(c) the necessary and available powers and functions to ensure compliance with data protection rights and promote awareness, including the ability, on its own initiative, to conduct investigations, request information from Data Controllers and Data Processors, issue warnings, order compliance, impose limitations or bans on processing and levy administrative fines;

(d) the head of the supervisory authority must be appointed through a transparent procedure by the Board and an appointment shall only end if (i) there is just cause; or (ii) the term of appointment has ended and has not been renewed; and

(e) sufficient resources and an annual budget which is approved by the Board , as well as an obligation to produce independently audited accounts and an annual report documenting its activities.

H. Remedies, liabilities and penalties

32. An effective data protection regime requires individuals, whose rights under data protection law are violated, to be able to pursue legal remedies and enforce their rights rapidly, effectively and without prohibitive cost. This involves the data subject having access to effective administrative and judicial redress, including compensatory damages, as a result of unlawful processing of his or her Personal Data. This should involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed. These sanctions can either be administrative in nature or levied by the courts.

33. ADGM proposes the supervisory authority be empowered by the Board to levy administrative fines, which are reviewable by the Courts. ADGM proposes to set an absolute cap on administrative fines under the New Regulations at USD $28 million, as this is commensurate with the maximum numerical cap under the GDPR, and recognises the importance of the rights and freedoms which the New Regulations will seek to protect. In cases of multiple breaches for the same or linked conduct, the fine will be assessed and the cap will apply on a cumulative basis.

Q8: DO YOU HAVE ANY COMMENTS ON THE PROPOSED ADMINISTRATIVE FINING CAP OF USD $28 MILLION.

I. Exemptions

Criminal law enforcement and national security purposes

34. The GDPR excludes law enforcement (broadly official bodies in respect of criminal offences and threats to public security) from its scope. Given that federal criminal law and laws governing national security apply in the financial free zones, ADGM does not have any power to monitor UAE federal criminal law enforcement, or national security agencies.

35. Accordingly ADGM proposes to exclude criminal law enforcement and national security from the New Regulations.

Exemptions to data subject rights

36. In addition, it is recognised that it can be onerous for Data Controllers to comply with the data subject rights obligations in certain limited circumstances. It may sometimes be the case that such rights cannot be complied with without undermining other important rights or societal or

governmental obligations of the Data Controller. The GDPR permits EU Member States to provide specific exemptions for Data Controllers from complying with their obligations in respect of data subject rights, provided the exemption "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure*" by which to achieve the relevant aim.

37. ADGM proposes to take the same approach and permit exemptions to the data subject rights obligations in the New Regulations where (at a high level) the data subject rights provisions would prejudice, including the following:

(a) prevention or detection of crime, apprehension or prosecution of offenders, or the assessment or collection of a tax or duty;

(b) information required to be disclosed by law or in connection with legal proceedings (including by court order);

(c) functions designed for public protection (including from financial loss due to dishonesty or malpractice, securing the health, safety and welfare of persons at work and regulating anti-competitive behaviour);

(d) the safeguarding of national security or defence;

(e) important economic or financial interests of ADGM;

(f) compliance with international obligations and standards (including the International Organisation of Securities Commissions), where inspection of Personal Data is required;

(g) information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;

(h) a person's ability to protect themselves from self-incrimination, to the extent that compliance with obligations under the New Regulations might expose them to proceedings for committing an offence (excluding perjury or an offence under the New Regulations themselves);

(i) disclosure which is prohibited or restricted by law (where it is specified in another regulation that such information cannot be disclosed e.g. tipping off in money laundering regulations);

(j) audit functions for supervising the quality of public accounting and financial reporting by administrative bodies;

(k) regulatory functions of public and administrative bodies;

Q9: DO YOU HAVE ANY COMMENTS ABOUT THE PROPOSED EXEMPTIONS TO DATA SUBJECT RIGHTS?

L. Entry into force

38. Adoption of the New Regulations will result in significant changes to ADGM's data protection regime and additional responsibilities for Data Controllers and Data Processors. ADGM recognises that entities that currently operate under the Existing Regulations will need time to upgrade their systems and practices for compliance with the New Regulations.

39. Accordingly, we propose the New Regulations include a 12-month transition period for existing establishments. This will give Data Controllers, Data Processors and the new supervisory authority time to adjust to the requirements of the New Regulations, and limit incidences of technical non-compliance due to changes in the legislation.

40. Establishments that are registered after the new Regulations come into effect will have 6 months from the effective date in which to adjust to the requirements of the New Regulations.

Q10: DO YOU HAVE ANY COMMENTS ABOUT THE PROPOSAL TO APPLY A 12-MONTH TRANSITION PERIOD TO EXISTING ESTABLISHMENTS AND A 6 MONTH TRANSITION PERIOD FOR NEW ESTABLISHMENTS?

PROPOSED AMENDMENTS AND REGULATIONS

- **Annex A Data Protection Regulations 2020**