ADGM Data Protection Regulations: What's New in 2021?

Krishna Jhala - Senior Counsel - Digital & Data
k.jhala@tamimi.com - Abu Dhabi

Ahmed Khairi
A.Khairi@tamimi.com - United Arab Emirates

Introduction

The new ADGM Data Protections Regulations 2021 (the **"New Regulations"**) were enacted on 11 February 2021 and published on 14 February 2021 thereby replacing the 2015 Data Protection Regulations ("**Old Regulations**"). The New Regulations will come into effect for existing entities on 14 February 2022 and for new entities (established after the New Regulations were published) on 14 August 2021. The New Regulations which are closely modelled on the EU's General Data Protection Regulation ("**GDPR**") set a new, stringent threshold for data protection in ADGM. The adoption comes only months after the DIFC, another financial free zone in the UAE enacted its own GDPR style data protection rules under DIFC Law No. 5 of 2020.

Capitalised terms used in this article are as defined under the New Regulations.

Introduction of Key Data Protection Principles

Similar to the GDPR, the New Regulations have introduced standalone principles of processing Personal Data such as lawfulness, fairness, and transparency, although existed under the Old Regulations, have been dealt with in detail. Additionally, the New Regulations includes heightened data protection obligations, greater transparency and accountability requirements, concepts of data protection by design and default, high risk processing activities, data protection impact assessments and appointment of data protection officer. The implementation of the New Regulations helps take ADGM one-step closer to achieving 'adequacy status' under the GDPR.

Lawful basis for Processing "Special Categories of Personal Data"

The New Regulations replace some of the broader basis for processing Special Categories of Personal Data, referred to as ("Sensitive Personal Data") in the Old Regulations with more specific grounds for processing. For instance, the New Regulations allow for processing Special Categories of Personal Data "*where it is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment law*". Mirroring the language of the GDPR, the New Regulations create a basis for processing of Special Categories of Personal Data where it is necessary for reasons of "*public interest in the area of public health, such as protecting against serious threats to health*…", or "pursuant to a contract with a health professional". This basis is in addition to what was provided under the Old Regulations which covered "the purposes of preventive medicine or medical diagnosis or the provision of care or treatment or the management of healthcare services".

The New Regulations also provides "substantive public interest" as a basis for processing of Special Categories of Personal Data. Examples of this include equality of opportunity, diversity at senior levels of organisation, the prevention of fraud, disclosures to public authorities regarding suspected terrorist financing, or suspected money laundering. It is important to note that the New Regulations completely remove the option of Processing Special Categories of Personal Data by way of obtaining a permit from the regulator.

The need for "Appropriate Policy Documents"

A unique provision in the New Regulations, is the explicit requirement to have an "appropriate policy document" in place when processing Special Categories of Personal Data for the following purposes: (i) in the field of employment law; and (ii) on the basis of a substantive public interest.

The Appropriate Policy Document (which may incorporate other documents by reference) should explain:

- how the Controller will comply with the principles of data processing;
- the Controller's policies regarding the retention and erasure of that Personal Data; and

Further, Appropriate Policy must be retained (until 6 months after the Controller carries out such processing), reviewed, updated and made available to the Commissioner on request.

Given the breath of what may come under the scope of "employment law" or "substantive public interest', as defined under the New Regulations, we anticipate that in order to achieve full compliance under the New Regulations, companies will not only be required to update their privacy policies, but will also need to

update their fraud policies, diversity and inclusion policies, employment policies, anti-money laundering policies, and any other policies falling within this scope.

Data Subject Rights

The New Regulations provide enhanced data subject rights. In addition to rights to access, erasure, blocking of data and right to object to processing provided under the Old Regulations, the New Regulations include: right to withdraw consent, right to the restriction of processing, right to data portability and right not to be subject to decisions made solely on automated processing, including profiling.

Further, the existing rights have been expanded such as the New Regulations provide two-month timeframe for responding to Data Subject's access requests. This initial period is further extendable by another one month. Where the erasure or rectification of Personal Data is not feasible for technical reasons, the Controller is required to inform the data subject at the time of collecting their Personal Data.

Controller must provide Data Subjects with information for meeting their transparency requirements:

- in a concise, transparent, ineligible and easily accessible form, particularly any information addressed specifically to a child; and
- in writing or electronically or if requested by the Data Subject, orally as long as that Data Subject has provided proof of identity.

Data subject rights provided under the New Regulations are similar to those provided under the GDPR and to an extent with the DIFC data protection laws.

Additional Security Obligations

While the Old Regulations include provisions as to the Controller's duty to ensure "security of processing", the New Regulations align with the GDPR, and introduce more rigorous and detailed obligations on both Controllers and Processors. Notably, the New Regulations impose an explicit duty on both Controllers and Processors to take into account the "state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks posed" when implementing technical and organisational measures. Examples of appropriate technical and organisational measures specified in the New Regulations include pseudonymisation and encryption of Personal Data, and the ability to restore access to Personal Data.

Further, the New Regulations introduce the GDPR principle of "Data Protection by design and by default" on Controllers, which had been absent from the Old Regulations. Essentially, "Data Protection by design" means that appropriate safeguards for Data Protection principles must be embedded into the complete life cycle of an organization's products, services, applications, business and technical procedures from the outset, when deciding on the means for processing, rather than through a reactive approach. Data Protection by default, in contrast, requires that only Personal Data which is necessary for each specific purpose of processing is processed, and for Personal Data to not be made accessible to an indefinite number of persons without the Data Subject's intervention.

Data transfers outside of ADGM

The New Regulations restricts data transfers to jurisdictions outside ADGM (i.e. third countries), as they often do not have the same level of stringency in data protection standards. Transfers to third countries is permitted under the New Regulations where: a) the ADGM Office of Data Protection has granted the third country with adequacy status, or an appropriate safeguard is in place. In the absence of an adequacy decision, one of the following safeguards must be in place: (a) standard contractual clauses (SCCs), as adopted by the ADGM Commissioner may be adopted. Note that the ADGM Commissioner has a fast-track procedure for approving the then current SCCs approved by the European Union; (b) legally binding, enforceable instrument between public authorities; (c) an approved code of conduct together with binding and enforceable commitments; (d) an approved certification mechanism together with binding and enforceable commitments; (e) Binding Corporate Rules to facilitate the transfer of Personal Data between members of a corporate group (reviewed and approved by the Commissioner); (f) Contractual clauses between Controller or Processor and Controller, Processor and Recipient of Personal Data or administrative arrangement.

Further, adequacy decisions granted by the ADGM Office of Date Protection are based on: (a) the rule of law, respect of individuals' rights, relevant legislation; (b) the existence and effective functioning of one or more independent supervisory authorities in the country receiving the data; (c) the international commitments of the countries receiving the data. Note the list of jurisdictions providing adequate level of protection under the Old Regulations hold good with the exclusion of USA after the Schrems II judgement.

Notifications of Data Breach

The Data Breach notification period under the New Regulations is the same as the Old Regulations (i.e. requirement to notify the Commissioner within 72 hours), if the notification of a breach was not made within 72 hours, reasons of delay must be stated to the Commissioner. Additionally the New Regulations include a duty to communicate Personal Data breach to the Data Subject where it is likely to result in a high risk to the rights of "natural persons" and to notify the Controller without undue delay after becoming aware of a Personal Data Breach.

The breach notifications to the Commissioner/data subject should include the following information:

- A description of the nature of the Personal Data Breach, including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the Personal Data Breach
- A description of the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Where notification is to the Data Subject, the notification should include practical recommendations to mitigate potential adverse effects and contain sufficient detail to allow him or her to take the necessary precautions.

High Risk Processing Activities & Data Protection

Impact Assessments

In aligning with the GDPR, and the DIFC DP Law, the New Regulations introduce the concept of High Risk Processing Activities, which include an obligation on the Controller to conduct a Data Protection Impact Assessment.

Whilst the term is undefined within the GDPR, the New Regulations provide a similar definition of High Risk Processing Activities to that found in the DIFC DP Law. Accordingly, High Risk Processing occurs where processing involves (i) a considerable volume of Personal Data, (ii) Processing which is likely to result in a high risk to the rights of Data Subjects, and (iii) where there is a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling and (iv) the Processing includes Special Categories of Personal Data, except where Processing of such data is required by Applicable Law. In contrast to the definition found under the DIFC Data Protection Law, the New Regulations exclude processing of Special Categories of Data where required by Applicable Law from the definition of High Risk Processing Activities.

Fines

The New Regulations imposes significant fines for data breach, with a strict cap not exceeding exceed USD 28 million. The administrative fines apply to both Controllers and Processors. In addition, Commissioner may issue a fixed penalty for non-payment of the Data Protection Fee on the Controller. The fine is up to 150% of the Data Protection Fee, or Renewal Fee, in addition to the Data Protection Fee or Renewal Fee. The fines are in addition of Data Subjects' rights to claim compensation.

For further information, please contact Krishna Jhala or Ahmed Khairi.