ARTICLE

What Companies Need to Know About the ADGM Data Protection Regulation

In February this year, the Abu Dhabi Global Markets (ADGM) passed the Data Protection Regulation (DPR2021), which bears a striking resemblance to the EU GDPR, and the U.K. GDPR specifically. The former legislation, dating back to 2015, was based on the Organization for Economic Co-Operation and Development (OECD) guidance, which was significantly different from GDPR's standards. What this means is that for companies operating in the ADGM, major regulatory changes are afoot.

US$28m

The maximum fine for each breach of the DPR2021 regulations

Companies already established in the region will have 12 months to become compliant with the new law, while new companies will have only six months. Considering that EU GDPR provided two years to prepare, and many companies still struggled to operationalise all the requirements on time, six to 12 months will be a difficult deadline to meet. Companies will need to prioritise the changes necessary for compliance with the new law, and follow a clear, actionable plan.

What does this mean for companies based in the ADGM, or planning on setting up in the ADGM?

Several key factors that were not included in the AGDM's previous data privacy requirements stand out in the new law. These include:

Accountability and governance

A major area of focus is the introduction of accountability and governance, particularly for data controllers, which were notably absent from the previous law. Data controllers will now be asked to prove that they have appropriate controls in place across the organisation to demonstrate that data privacy is taken seriously. This includes a mandate to appoint a Data Privacy Officer (DPO), which may be an employee or an outsourced expert. Companies will also be required to conduct and document data privacy impact assessments

(DPIAs), keep a record of processing activities and provide documentation of data subject access request (DSAR) processes. Cross-border data transfers will also be regulated, and for the first time, companies will have the option of governing data transfers via binding corporate rules (BCRs). Additional governance controls mandated in DPR2021:

- Data privacy policies
- Employee contracts
- Employee awareness and training
- Evidence that privacy by default and privacy by design are embedded in the company
- Documented evidence of security standards and protocols used
- Vendor due-diligence evidence

Accountability requirements are less onerous for companies with five or fewer employees. However, the vast majority of companies in the ADGM will be required to adhere to the new standards.

Territorial scope

The scope of the application of this law has also changed. Unlike GDPR, which governs all qualifying organisations doing business in the region, DPR2021 applies to any company *established* in the ADGM, or to data processors processing data either in the ADGM, or on behalf of an ADGM data controller, regardless of whether the processor is in the ADGM or not. The scope of the law is also applicable to any natural, legal person regardless of location or nationality, which does give it an extra-territorial element, like GDPR.

Data subject rights and automated profiling

DPR2021 introduces a new right for data subjects not to be subject to automated processing or profiling that significantly affects that person or carries legal implications. This is particularly relevant to the ADGM, which has created a thriving fintech hub and actively champions the development of a sustainable and vibrant fintech ecosystem. Although many companies in the fintech space are start-ups or small-to-medium enterprises, a sizeable proportion of them will be employing technologies that leverage AI and machine learning to potentially automate data processing and profiling.

The controller must also, on request, provide a copy of the data subject's data to them in a concise, transparent, intelligible, and easily accessible form, in writing, electronically or verbally. As many organisations experienced with GDPR, fulfilling these requests can be extremely time consuming and resource intensive.

Data portability

Data subjects will also now have the right to transfer their data to a third party, a requirement which was directly ported from GDPR. This will require companies to transfer data on request from the data subject, in a standard, machine readable format, to another controller who may well be a direct competitor. Supporting this functionality will likely involve system, process and/or template changes.

Timeline for reacting to DSARs

The ADGM will allow two months for responding to a DSAR, with the potential for a one-month extension under certain circumstances. This timeline departs from the standards of GDPR and Dubai International Financial Centre (DIFC), and may be more pragmatic, particularly for SMEs. However, the regulator has been very clear in discouraging repeated extension requests and indicating that companies will be questioned if they are found to be abusing the allowance.

Consent-based processing

In DPR2021, consent now needs to be "a freely given, specific, informed and unambiguous indication of the data subject's wishes" through a clear affirmative action. Pre-ticked boxes or inactivity no longer constitute consent, and to be informed, the data subject should be aware of the identity of the controller and the purposes for which it is intended their personal data will be processed. The controller must also be able to demonstrate that the data subject has consented and maintain a register of that valid consent.

The data subject now also has the right to withdraw consent at any time, and it must be as easy to withdraw consent as it is to give consent. This has serious operational ramifications for many organisations that share personal data with various processors. Organisations must now consider how their website collects consent to deploy cookies, or the consent mechanism being used by customers to opt in or opt out of marketing communications.

And finally, to be "freely given" the data controller must consider whether the data subject has a genuine or free choice or is unable to refuse or withdraw. With DPR2021, in the employer/employee relationship, consent has now become a legal basis that needs thorough consideration due to the intrinsic imbalance of employer/employee

relationships. This makes the use of consent as a lawful basis increasingly challenging. Alternative lawful bases for processing of personal data, like performance of a contract or the controller's legitimate interest, may now become more suitable.

Cross-jurisdiction transfers

International transfers of data are a hot topic in the Middle East. This is not only because of the unfolding implications of the Schrems II case, but because many organisations in the Middle East are already subject to data sovereignty or data residency challenges at a national or industry level.

The language used by the ADGM states that, in the absence of an adequacy decision, a controller or processor may transfer personal data outside the ADGM only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These typically tend to be either standard contractual clauses (SCCs) or BCRs.

The countries deemed adequate under the ADGM are now identical to those considered adequate by both GDPR and DIFC, with the addition of DIFC as an adequate jurisdiction. Note that UAE mainland and other freezones are not considered adequate jurisdictions, so data transfers to those will need to be handled with care. As with all international data transfers, a risk assessment should be performed, and SCCs put in place before any transfer can occur. Organisations transferring data within their own company, or group of companies, will now be suitably covered under the use of BCRs.

Interaction with the regulator

In addition to the new requirement for all data controllers and processors to register with the ADGM Office of Data Protection (and pay the relevant fee), companies are also required to engage with the regulator whenever a DPIA reveals a high risk to the rights of the data subject, or if sensitive data is being processed. Like GDPR, there is an additional requirement to report any data breach that might impact the rights of a data subject within 72 hours.

Additionally, intra-company international data transfers utilising BCRs as the relevant control mechanism need to be reviewed and approved by the regulator before enactment.

Fines and penalties

DPR2021 has a maximum fine of US$28 million for each breach of the regulations. This is substantially lower than the 4% of global revenue available under GDPR, but significantly higher than the US$120,000 available under the DIFC law. These fines are in addition to data subjects' rights to claim compensation if they have suffered material or non-material damage as a result of a contravention of these regulations. The data subject may then be entitled to compensation from the controller or processor for the damage suffered, with a case brought in court.

Summary

For companies that are already established in the ADGM and compliant with the 2015 law, compliance with the new law will not require a complete overhaul, but work will still need to be done. Organisations that have been operating under the DIFC Data Privacy Law 2020 or GDPR will have a heavier lift but will still be able to fulfil requirements on time if they take swift and targeted action. It will be key to ensure programmes are built with flexibility in mind, so that they can adapt to meet additional changes to data privacy law on the horizon in the ADGM, the broader Middle East region and globally.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

BEN CREW
Senior Director, Information Governance and Privacy
+971 (0)50 286 7553
ben.crew@fticonsulting.com