BREMER

DIFC and ADGM Data Protection Regimes

Client briefing | DIFC and ADGM data protection regulations
Location | UAE
Date | 15 January 2026

The UAE has developed a multi-layered data protection framework that reflects both its federal legal system and the autonomy of its financial free zones. Businesses operating in the UAE must be aware that data protection obligations—including breach notification requirements—vary depending on where an entity is established and how personal data is processed.

The UAE Federal Personal Data Protection Law established the baseline data protection regime applicable across the onshore UAE effective 2 January 2022. It is broadly inspired by the EU General Data Protection Regulation (GDPR), and is designed to regulate the processing of personal data relating to identifiable natural persons.

The law applies to:

- data controllers and processors established in the UAE—including the UAE freezones, except the the financial free zones; and
- foreign entities that process personal data relating to individuals in the UAE.

Entities established in the UAE financial freezone—the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM)—are not subject to the Federal Personal Data Protection Law but instead are governed by specific regulations of the financial freezones. Both the DIFC and ADGM data protection regimes are built around three core principles:

- prerogative of protection of individuals rather than businesses;
- accountability of controllers, including proactive risk assessment and

Unlike some sector-specific cybersecurity rules, these regimes are not concerned with operational resilience or commercial harm as such, but with whether a security incident has compromised personal data and created a risk to individuals' rights and freedoms. The definition is intentionally broad and captures both cybersecurity incidents (such as hacking, ransomware attacks, or phishing) and operational incidents (such as misdirected emails, loss of devices, or unauthorized internal access).

Scope of application

Like the UAE Federal Personal Data Protection La, both the DIFC and the ADGM data protection regimes apply to:

- data controllers and processors, incorporated or registered in the DIFC or ADGM; and
- entities established outside the freezones where they process personal data in the context of activities carried out in the DIFC or ADGM; and
- entities established outside the freezones in connection with services they offer to individuals or entities within the freezones.

Personal data breach

Under both regimes, a personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is transmitted, stored, or otherwise processed. The focus of the analysis is not on the cause of the incident, but on whether personal data has been compromised and whether that compromise creates a risk to

obligations are similar in both regimes, they do differ in certain aspects.

In the ADGM, controllers are required to notify the ADGM Commissioner of Data Protection without undue delay and, where feasible, within 72 hours of becoming aware of a personal data breach. Where notification is made late, the controller is expected to document and justify the delay. This prescriptive timeframe places a strong emphasis on early internal escalation, rapid investigation, and preparedness.

By contrast, the DIFC Data Protection Law requires controllers to notify the DIFC Commissioner of Data Protection as soon as practicable in the circumstances where the breach compromises the confidentiality, security, or privacy of personal data. Although no fixed deadline is specified, the expectation is that notification will be made promptly, and any unjustified delay may be taken into account by the Commissioner when assessing compliance or determining enforcement action.

Notification to affected individuals

In addition to regulatory notification, both regimes require notification to affected individuals where the personal data breach is likely to result in a risk, to their rights or freedoms. This assessment is risk-based and requires organizations to evaluate the potential impact of the breach on individuals, taking into account factors such as the nature and sensitivity of the personal data involved, the ease of identifying affected individuals, the severity and likelihood of potential harm, and whether effective mitigation measures, such as encryption, were in place. Where notification to individuals is required, it must be made without undue delay and in clear and plain language, enabling individuals to understand the nature of

Obligation of processors

Processors also play a critical role in the breach notification framework under both regimes. While processors are not required to notify the regulator directly unless they act as controllers in their own right, they are required to notify the relevant controller without undue delay after becoming aware of a personal data breach. This obligation is essential to enabling controllers to meet their regulatory notification timelines, particularly under the ADGM regime, and should be clearly reflected in data processing agreements and outsourcing arrangements.

Even where a personal data breach does not trigger notification to the regulator or affected individuals, both the DIFC and the ADGM require controllers to document all personal data breaches, including the facts surrounding the incident, its effects, and the remedial actions taken. These records form part of the accountability framework and may be requested by the relevant authority in the context of audits or investigations. It is also important to note that neither regime imposes notification obligations in respect of breaches involving purely corporate or commercial data, such as trade secrets or confidential business information, unless such information includes personal data relating to identifiable individuals. In practice, however, many corporate documents contain personal data, meaning that incidents initially perceived as purely commercial may still fall within the scope of the notification regime.

Documentation and accountability

Even where a personal data breach does not trigger notification to the regulator or affected individuals, both the DIFC and the ADGM require controllers to document all personal data breaches, including:

- the assessment of risk to individuals; and
- the remedial and preventive actions taken.

These records form part of the accountability framework and may be requested by the relevant authority in the context of audits or investigations.

What falls outside the notification scope

Neither regime imposes notification obligations in respect of breaches involving purely corporate or commercial data, such as trade secrets or confidential business information, unless such information includes personal data relating to identifiable individuals. In practice, however, many corporate documents contain personal data, meaning that incidents initially perceived as purely commercial may still fall within the scope of the data protection notification regime.

Key Takeaway

The DIFC and the ADGM data protection regimes impose sophisticated, personal-data-focused breach notification obligations that require organizations to move quickly from incident detection to legal assessment and regulatory engagement. Businesses should ensure that suspected breaches are escalated quickly so that an early assessment can be made as to whether personal data is involved and whether notification obligations are triggered, particularly given the prescriptive timelines under the ADGM regime.

Clear internal incident response procedures, aligned across legal, compliance, and IT teams, are essential to enable timely and well-reasoned notification decisions. Organizations should also ensure that data processing and outsourcing agreements include robust obligations on incident and the assessment undertaken is critical to demonstrating compliance with the DIFC and the ADGM accountability requirements.

Mariem Saad

Senior Associate

mariem.saad@bremerlf.com

Mariem is a senior associate of the region law firm BREMER and part of the firms Mergers & Acquisitions (M&A) team. She advises international corporates on mergers & acquisitions and joint venture transaction including as well as ECA backed export and project finance transactions in the Middle East. She works in English and Arabic languages.

NICOLAS BREMER

Partner

nicolas.bremer@bremerlf.com

Nicolas is a partner and attorney with the regional law firm BREMER where he heads the firm's Antitrust & Merger team. He oversees the firm's Riyadh and Cairo representations and has extensive experience in advising international and domestic clients on merger control and antitrust matters in Saudi Arabia, Kuwait, Egypt and the wider Near and Middle East. He works in English, Arabic and German.