White Label Consultancy

GCC Mid-Year Review

Mapping the Horizon

July 2025

Mapping the Horizon

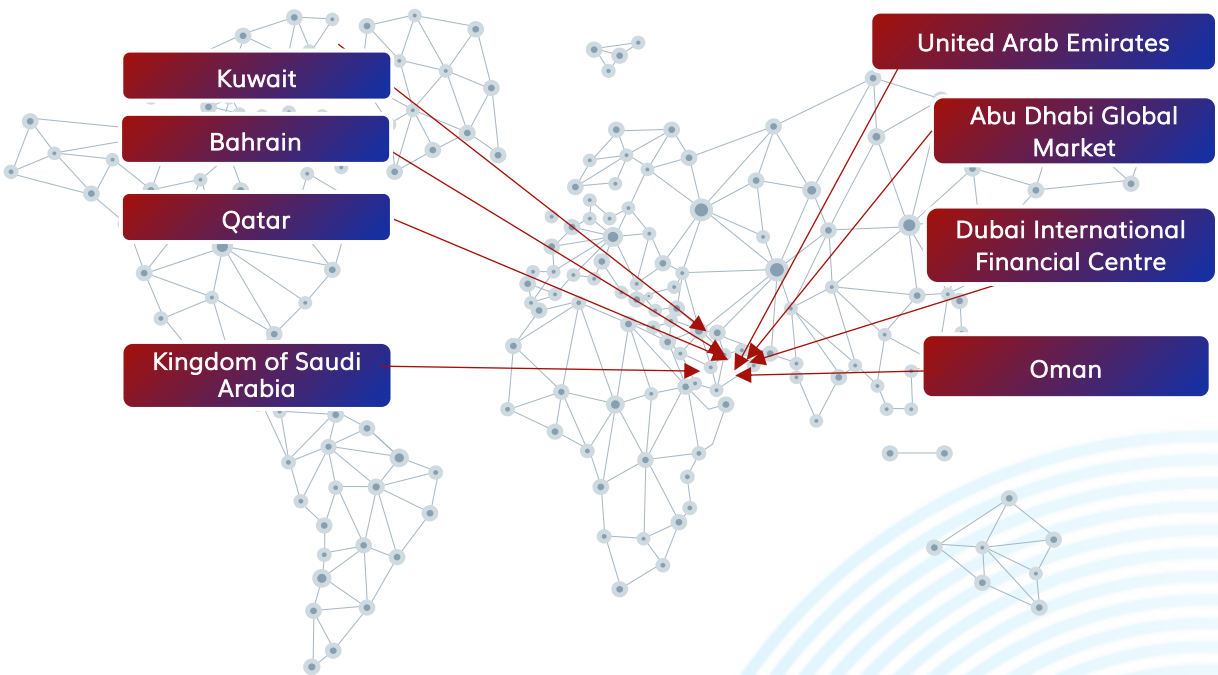
In the first half of 2025, countries in the Gulf Cooperation Council (GCC) have made significant strides in proposing and refining robust data privacy frameworks, aligning themselves with international best practices while tailoring regulations to their unique contexts.

From comprehensive proposals to evolving enforcement practices and a growing emphasis on cybersecurity, we provide below a quick look at the landscape of data protection across the GCC, with a view on what can be expected in the second half of the year.

What do organisations need to know?

For organisations operating in or engaging with companies in the GCC, understanding these evolving regulations is crucial as these can significantly impact compliance approach and business strategy.

This article will delve into the latest developments, offering a timely overview of how the region is safeguarding personal data in an increasingly interconnected world and what organizations need to know to navigate this complex yet vital landscape successfully.



Kingdom of Saudi Arabia

On 21 April 2025, the Saudi Data and Artificial Intelligence Authority (SDAIA) opened public consultation on draft *amendments to the Implementing Regulation of the Personal Data Protection Law (PDPL).*

Key proposed amendments include:

1. Requiring the language in privacy policies to be consistent with the language customarily used for providing the services or products to the data subjects whose data is being processed.
2. Removing the requirement of clearly identifying the sender in every direct marketing message.
3. Requiring the controller to document the appointment of Data Protection Officer (DPO) and notify the regulator in the Competent Authorities' Platform.
4. Specifying the types of data controllers required to register in the National Register. These data controllers include those whose primary activity is based on processing of personal data; who process sensitive data; and those who process personal data of data subjects lacking legal capacity.
5. Requiring controllers to respond within 10-business days (from receipt) to requests coming from the SDAIA regarding PDPL compliance.

Why is this important?

The amendments, particularly those concerning the documentation of DPO appointments and registration requirements for certain data controllers, create new administrative and reporting mandates that organisations must address.

United Arab Emirates

In late May 2025, the governments of the United Arab Emirates (UAE) and the United States launched the "US-UAE AI Acceleration Partnership." The framework includes the *launch of a 1-Gigawatt (GW) artificial intelligence (AI) data center* as part of a 5GW UAE-US AI technology cluster in Abu Dhabi.

Why is this important?

This development positions the UAE as a pivotal global hub for AI, signaling a significant move towards AI infrastructure.

White Label Consultancy

Dubai International Financial Centre (DIFC)

In July 2025, the Dubai International Financial Centre Authority (DIFCA) announced that it has enacted amendments to the Data Protection Law, DIFC Law No. 5 of 2020 (DPL), through the DIFC Laws Amendment Law No. 1 of 2025. The Amendment Law was enacted on 8 July 2025 and came into effect on 15 July 2025.

Key changes include:

1 *Clarification and extension of the DPL's scope.* The proposal clarifies that the DPL applies to:

(i) a DIFC-registered entity that processes personal data, regardless of where the processing takes place;

(ii) any entity, regardless of its place of incorporation, that processes personal data in the DIFC as part of stable arrangements.

These amendments are intended to align the extra-territorial scope of the DPL with the GDPR and other comparable laws, and remove ambiguity on the applicability of the DPL.

2 *Cross-Border Transfer Rules*

The amendment introduces rigorous safeguards for data disclosures to public authorities and third parties.

3 *Private right of action for aggrieved data subjects*

The amendment allows data subjects to directly seek judicial redress at the courts for alleged violations of the DPL, without need for a prior investigation or action by the Commissioner. This approach is seen to empower the DIFC Courts to make compensatory orders for "damage" involving not only financial loss, but also distress and other non-financial harm.

4 *Heightened Accountability & Compliance Burdens*

The amendments impose higher penalties, particularly for high-risk processing activities.

(i) Failing to complete Annual Controller Assessment: Fine of $25,000.

(ii) Failing to carry out a DPIA prior to High-Risk Processing: Fine is increased from $20,000 to $50,000.

(iii) Failing to comply with the requirements on data sharing: Fine is increased from $10,000 to $50,000.

Next steps

This is a significant development that impacts all entities operating within the DIFC jurisdiction. We strongly advise companies to undertake a comprehensive review of their operations and legal frameworks to ensure full compliance with the DIFC Amendment Law.

White Label Consultancy

Eye on Events:

Dubai and DIFC has been selected by the Global Privacy Assembly to host the *Global Privacy Assembly Conference in 2026*.

The Global Privacy Assembly was established in 1979 as the International Conference of Data Protection and Privacy Commissioners. Today, it connects 130 data protection and privacy authorities across the globe.

The event is expected to draw data protection authorities, non-governmental organisations, and technology companies to Dubai.

Abu Dhabi Global Market (ADGM)

On 30 April 2025, the Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market (ADGM) issued a consultation paper inviting public feedback on its proposal to introduce specific cyber risk management requirements for regulated firms (Cyber Risk Rules).

The proposed Cyber Risk Rules include:

1. Requirement for firms to identify and assess their cyber risks, establish and maintain a Cyber Risk Management Framework (CRMF) that appropriately addresses those risks, put in place governance and systems and controls, undertake ongoing monitoring and reporting, and manage and control cyber incidents.

2. Requirement to notify material cyber incidents to the FSRA immediately, no later than 24 hours after the firm becomes aware of an incident, notwithstanding weekends or public holidays

Why is this important?

The proposed Cyber Risk Management Rules are intended to align the FSRA with international best practices in combatting financial crime.

Next steps

Following public consultation, the FSRA will consider whether any modifications are required and will enact the proposed amendments.

White Label Consultancy

Kuwait

In February 2025, the one-year grace period for compliance with Kuwait Administrative Decision 26 of 2024 Concerning the Issuance of the Data Privacy Protection Regulation *(Kuwait Data Protection Regulation)* issued by the Communications and Telecommunications Regulatory Authority (CITRA) officially ended.

Under Article 11 of the Kuwait Data Protection Regulation, the grace period, which began on the date of its publication in the Kuwait Official Gazette, allowed service providers or such parties licensed to own public communications networks to adjust their practices to comply with the new regulations.

A note on scope:

The Kuwait Data Protection Regulation applies only to service providers that offers communications and information technology services in Kuwait including those who:

1. Provide, manage, establish, or create public communications networks.
2. Operate websites, smart applications, or cloud computing services.
3. Collect or process personal data (or direct others to do so on their behalf) through owned or utilized data centers.

Sultanate of Oman

Oman extended the *grace period for compliance with the Oman Personal Data Protection Law (PDPL) Executive Regulations (Ministerial Decision 34/2024)*, to 05 February 2026.

Eye on AI:

In May 2025, the Oman Ministry of Transport, Communications, and Information Technology (MTCIT) issued a *general policy for the safe and ethical use of artificial intelligence (AI) systems*. The policy establishes ethical principles and technical controls for the AI system lifecycle, focusing on transparency, fairness, accountability, inclusiveness, and privacy, and ensures human intervention in sensitive decisions to mitigate bias and misuse risks.

Why is this important?

Public and private sector entities developing and using AI systems are obligated to implement effective governance measures, such as periodic performance evaluations, documentation of decision-making processes, and submission of compliance reports upon request.

White Label Consultancy

Qatar

The *Qatar National Data Privacy Office (NDPO)*, part of the National Cyber Security Agency, issued a "legally binding decision" against a company in the Qatar ICT sector for violations of the provisions under the Qatar Data Privacy Protection Law (PDPPL) relating to consent, ensuring data accuracy, data protection safeguards, and ensuring compliance of third-party processors.

Why is this important?

This decisive action by Qatar NDPO highlights its commitment to actively enforcing data privacy regulations. The decision also sets a crucial precedent within Qatar's digital economy.

Bahrain

While the Bahrain Personal Data Protection Law came into force in 2019 after one year from its publication in the Bahrain Official Gazette, 2025 sees continued efforts by the Personal Data Protection Authority in its implementation, particularly with Data Protection Officer (DPO) requirements in sectors such as in finance, baking, education, health and telecommunications.

What can be expected in the second half of the year:

Amendments to data protection laws will be formally enacted.
For organisations operating within the GCC, this will necessitate review and adjustment of compliance frameworks, particularly those with operations in multiple jurisdictions.

Accelerated AI Governance. We expect jurisdictions like the UAE to continue to strategically integrate AI into its national strategy. In response to this, organisations must review how to integrate AI governance into its operations.

Heightened cybersecurity rules in critical sectors. As the threat landscape evolves in critical sectors (finance, energy and others), organisations must strengthen existing controls, and proactively review their incident response plans.

White Label Consultancy

White Label Consultancy

We understand that the fast-paced and ever-evolving digital regulatory landscape presents challenges for awareness and compliance for each organisation.

White Label Consultancy is committed to supporting you navigate this critical and dynamic field with actionable guidance and practical insights, ensuring strategic advantage for you and your business.

Thank you!

We are here to assist you with any concerns or queries you may have regarding privacy protection.

If you have any questions regarding privacy, please contact us at hello@whitelabelconsultancy.com.

or send us your inquiry at

https://whitelabelconsultancy.com/contact/ .

White Label Consultancy