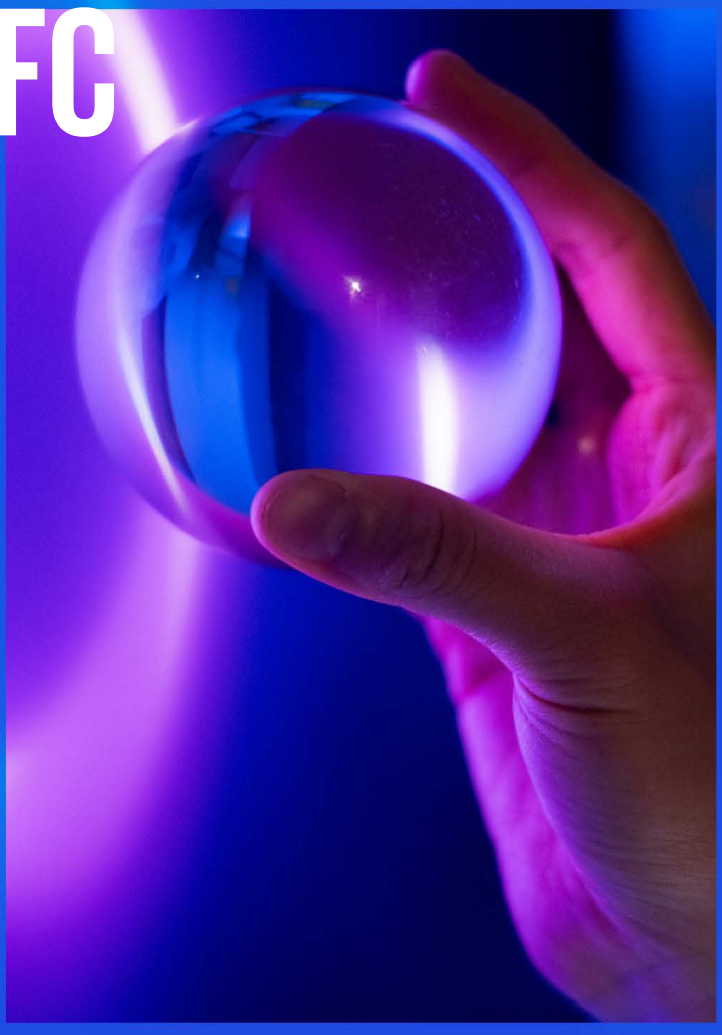
Strengthening data privacy and protection in DIFC

What the 2025 amendments mean for your business



KPMG. Make the Difference.

September 2025

Introduction

Over the past few years, the United Arab Emirates (UAE) has made meaningful progress in strengthening its data protection landscape. This includes the introduction of national-level Personal Data Protection Law (PDPL) and the establishment of data privacy and protection regulations within key financial free zones such as the Dubai International Financial Centre (DIFC) and Abu Dhabi's International Financial Centre (ADGM).

As part of this continued development, the DIFC has updated its Data Protection Law No. 5 of 2020 to reflect emerging global practices and address practical challenges faced by businesses. The latest set of amendments, introduced through Amendment Law No. 1 of 2025 and effective from 15 July 2025, bring enhancements across several areas including individual rights, cross-border processing, regulatory scope, and compliance obligations. These updates aim to provide greater clarity, reinforce accountability, and ensure that the DIFC continues to offer a robust and future-ready data protection framework for organizations operating within its jurisdiction.

Regulatory context

Since its enactment in 2020, the DIFC Data Protection Law has played an important role in shaping data protection practices in the region. It draws from international standards such as the EU-GDPR and aims to promote strong privacy principles. In recent years, the DIFC has continued to strengthen its position as a leading center for data protection, with the commissioner's office encouraging greater adoption of privacy practices, transparency, and accountability across the business community.

The latest set of amendments, developed through a public consultation earlier this year, reflects the DIFC's efforts to keep pace with evolving business needs and global developments. These changes address practical challenges related to the use of artificial intelligence, international data transfers, and individual rights, providing further clarity for organizations working with personal data.

Key amendments

Amendment area	What has changed	What it means for organizations
Article 64A **Introduction to privacy right of action**	Individuals now have the right to bring legal claims directly before the DIFC courts if their data protection rights have been violated. They are no longer required to first file a complaint with the DIFC commissioner. These claims can include both financial loss and non-financial harm, such as emotional distress.	Organizations must be prepared for potential legal claims from individuals in addition to regulatory investigations. It is important to maintain clear documentation, evidence of compliance efforts, and robust internal procedures to demonstrate accountability. Legal, privacy, and compliance teams should work together to ensure readiness for dispute resolution and response.
Article 6 **Clarification on scope of law**	The law now explicitly applies to entities incorporated in the DIFC, regardless of where their data processing takes place. It also applies to controllers and processors outside the DIFC if they process personal data through a stable business arrangement in the DIFC or on behalf of DIFC-based entities.	Businesses outside the centre that offer services to DIFC entities or act as service providers may now be directly subject to the law. This means that non-DIFC vendors, especially sub-processors, must assess their obligations and ensure alignment with DIFC compliance requirements. Organizations should review contracts and data flows to determine if these changes apply to their operations.
Article 28 **Changes to data disclosure rules to public authorities**	The law previously required that public authorities requesting personal data had to ensure protection of data subject rights. This requirement has been removed. Instead, the responsibility now lies with the controller or processor to confirm that the request is lawful, proportionate, and necessary before disclosing any data.	Organizations must take extra care when receiving requests from government authorities. A documented process for assessing the legitimacy, necessity, and proportionality of such requests should be established. This includes consulting legal teams when required and maintaining an audit trail of all disclosures to public authorities.
Article 19, 20 and 28 **Higher financial penalties introduced**	The DIFC has increased administrative fines for certain non-compliance areas: • Failing to conduct and submit an annual assessment can result in a fine of USD 25,000. • Failing to carry out the required DPIA can lead to a fine of USD 50,000. • Not meeting obligations for handling data disclosure requests from public authorities may also result in a fine of USD 50,000.	These penalty increases reflect the DIFC's intent to enforce compliance more rigorously. Organizations must prioritize timely completion of the annual assessment and ensure DPIAs are carried out for all high-risk processing. Governance frameworks should be reviewed to verify that these activities are well documented and assigned to responsible teams.
Article 20 **Reinforcement of DPIA obligations**	While DPIAs were already a requirement for high-risk processing activities, the increased penalty and clearer expectations reinforce their importance. The law emphasizes the need to assess and mitigate risks to individuals before processing begins.	Organizations must review their existing DPIA process to ensure it captures relevant risks and includes appropriate mitigation actions. Use cases involving artificial intelligence, biometric processing, automated decision-making, or large-scale profiling should be prioritized. Privacy teams should work closely with IT, analytics, and business functions to ensure early involvement in new projects.

Strategic considerations

The amendments reflect a broader accountability shift. While they maintain core DIFC data protection principles, the enhanced litigation and compliance landscape necessitates concrete changes in how organizations approach privacy operations.

1. Litigation readiness and data governance

Organizations should:

- Review privacy notices and internal breach response procedures.
- Align legal, risk, and compliance teams to handle civil data claims.
- Update DPO role definitions and reporting structures to ensure independence.

2. Public authority engagement protocols

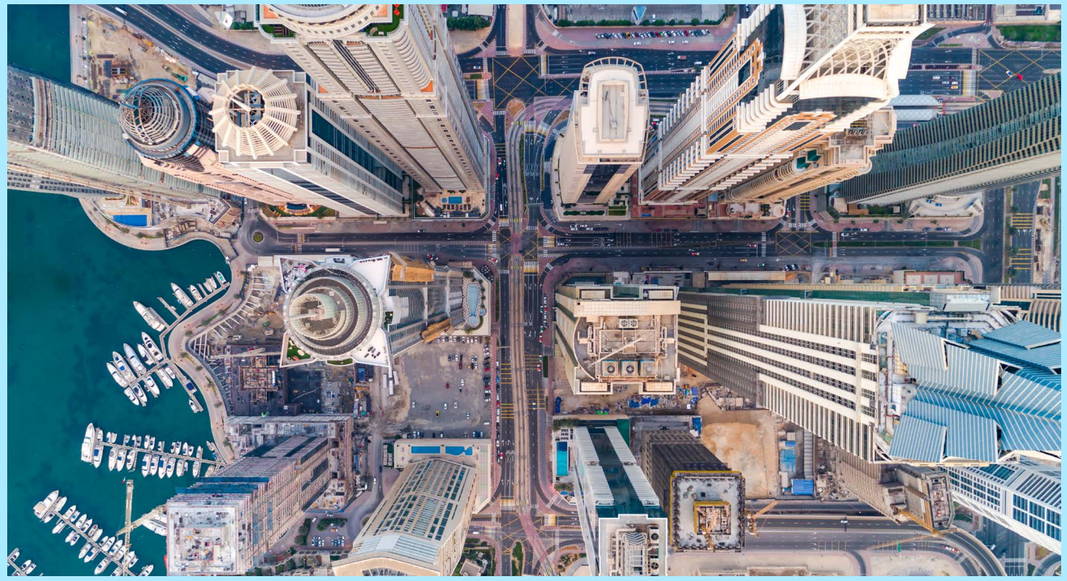
- Establish internal standard operating procedures (SOPs) for handling requests from public authorities.
- Build proportionality assessments into the approval workflow.
- Log and periodically review disclosures to mitigate audit risk.

3. Cross-border processing and vendor oversight

- Conduct updated RoPA (records of processing activities) to reflect all DIFC-linked processing.
- Reassess existing data processing agreements and transfer mechanisms.
- Ensure vendors outside the DIFC understand and meet local obligations.

4. Operational compliance uplift

- Conduct or refresh DPIAs for high-risk processing (AI, biometrics, etc).
- Implement and submit the required annual assessment on data protection compliance.
- Document all changes in an updated compliance framework to withstand regulator and court scrutiny.



How KPMG can help

The recent amendments to the DIFC Data Protection Law introduce both strategic opportunities and new compliance responsibilities for organizations. With increased regulatory scope, enhanced individual rights, and a stronger enforcement regime, businesses must act decisively to assess their readiness and reduce their exposure to legal and financial risk.

At KPMG, we help organizations navigate these evolving requirements through a combination of advisory support, technical expertise, and implementation capabilities. Our services are designed to enable both compliance and long-term operational effectiveness.

Our service offerings

1. **Gap assessment and compliance readiness**
   - Conduct detailed reviews to identify gaps in current privacy practices against updated DIFC obligations.
   - Assess readiness for private right of action exposure and develop action plans to address deficiencies.
   - Review and align data protection policies, governance structures, and accountability mechanisms.

2. **Data protection impact assessments (DPIAs)**
   - Provide tailored DPIA templates and support for high-risk processing activities such as AI, biometrics, and profiling.
   - Facilitate stakeholder workshops to assess privacy risks and document mitigation strategies.
   - Help embed DPIA requirements into project and change management lifecycles.

3. **Cross-border processing and vendor risk management**
   - Review processor and sub-processor arrangements, especially where services are provided from outside the DIFC.
   - Assist in updating contracts and data transfer mechanisms to reflect the expanded scope of applicability.
   - Support organizations in meeting their obligations as both data controllers and processors.

4. **Public authority disclosures and legal risk**
   - Design protocols and validation checklists for assessing government or regulatory data requests.
   - Assist with developing internal guidance, recordkeeping procedures, and legal review workflows.
   - Advise on balancing legal compliance with protection of data subject rights.

5. **Litigation and enforcement preparedness**
   - Develop strategies to prepare for and manage potential private legal claims by individuals.
   - Support organizations in documenting their data protection efforts to demonstrate compliance in case of an audit or legal challenge.
   - Advisory support to manage interactions with the DIFC Commissioner and DIFC Courts.

6. **Advisory annual assessment**
   - Guide organizations through the process of completing their annual assessment in line with Article 19.
   - Provide templates, review support, and reporting insight to meet documentation and submission requirements.

7. **Training and awareness**
   - Deliver customized training sessions for leadership, legal, risk, and operational teams on the implications of the law.
   - Help establish a privacy-aware culture through targeted communication campaigns and ongoing education programs.

KPMG's cross-functional team of cyber and privacy professionals and technology specialists is well-positioned to support DIFC-licensed entities and their partners. Whether your organization is just starting to build its compliance framework or looking to update it in light of the July 2025 amendments, we can help you achieve both regulatory alignment and business confidence.

Looking ahead

The 2025 updates to the DIFC Data Protection Law mark an important step forward for data privacy in the region. These changes introduce new rights for individuals, clearer responsibilities for organizations, and a stronger focus on accountability.

Instead of seeing this as just another compliance requirement, businesses can use this opportunity to strengthen how they manage personal data and build greater trust with customers, employees, and partners. With the right guidance and planning, meeting these requirements can also support long-term business success.

At KPMG, we are here to help organizations understand what these changes mean and take the right steps to build privacy programs that are effective, practical, and ready for the future.

Contacts

Timothy Wood
Partner, Digital and Innovation - Cyber & Privacy
UAE and Oman
KPMG Middle East
timothywood@kpmg.com

kpmg.com/sa
kpmg.com/ae
kpmg.com/om

Publication name: Strengthening data privacy and protection in DIFC
Publication number: 5667
Publication date: September 2025