waystone | Compliance Solutions

Do Representative Offices need to comply with the DIFC Data Protection Law?

May 19, 2026

In the course of our work, we occasionally encounter the view that the Dubai International Financial Centre ('DIFC') Data Protection Law ('DPL') is not applicable to representative offices that do not have clients. While understandable, this interpretation is not correct under the DIFC framework and can create compliance exposure.

The DIFC DPL applies based on personal data processing, not commercial activity.

Whether an entity has clients, generates revenue, or conducts regulated business is irrelevant for DPL applicability.

Representative offices **do** process personal data

In practice, almost all representative offices process personal data, including:

- employee, secondee, and contractor data
- directors', officers', and authorised signatories' personal information
- CVs and recruitment records
- visitor logs, access controls, security passes, and CCTV footage
- business contact details within global group structures.

Each of the above triggers obligations under the DIFC DPL.

"No clients" is not a regulatory defence

The DIFC Commissioner of Data Protection has made clear through guidance and enforcement activity that **entity type or perceived low risk does not create an exemption**. During inspections or enquiries, representative offices are expected to demonstrate compliance on demand.

Where an office cannot do so, regulators will proceed on the assumption that the entity is non-compliant, not merely unaware.

Consequences of non-compliance

Failure to comply with the DPL can result in formal regulatory investigations, administrative fines and Increased scrutiny during licence renewals and future regulatory interactions.

In our experience, enforcement action is typically triggered when an organisation has no documented compliance at all — which is exactly the position many representative offices currently find themselves in.

Compliance must be proportionate – but it must exist

While the DIFC takes a pragmatic approach, it does not accept a “do nothing” stance. Even the smallest representative office is expected to have:

- clear visibility over what personal data it processes
- documented governance (policies, notices, accountability)
- lawful cross-border transfer arrangements (common in group structures)
- evidence of staff awareness and basic controls.

These measures are baseline requirements, not best practice.

How we can help you

Many representative offices rely on existing GDPR frameworks, which **do not** automatically meet DIFC DPL requirements. We can review your current arrangements specifically against the DIFC DPL and implement any required localisation and support with your ongoing data protection obligations, to ensure regulatory compliance in the DIFC. Please reach out to our data protection team to arrange an initial discussion.

Contact us →