DIFC DATA PROTECTION REGULATION 10: COMPLIANCE AND ENFORCEMENT

REGULATION 10

Regulation 10 is an initial step toward further implementing privacy by design and default in your organisation's advanced technology, including AI Systems. This definition aligns with global standards such as the Organisation for Economic Co-operation and Development ('OECD') guidelines regarding AI systems capable of processing personal data for purposes primarily that are human-defined or human-approved. Additionally, Regulation 10 covers:

Principles - AI systems should incorporate principles such as ethics, fairness, transparency, security, and accountability from the design phase.

Clear and explicit notices - Applications utilising AI systems must provide a clear and explicit notice at the time of initial use or access, including potential impact of the AI system's use on individuals' rights, if any.

Evidence - Evidence of both technical and organisational measures must be provided to affected parties, relevant entities, or the regulator.

Register - Firms are also required to maintain an AI register of use cases.

CERTIFICATION OF SYSTEMS

DIFC DPL Regulation 10 is of particular importance when personal data is processed for use in, or to facilitate the learning processes of, any AI systems. The requirements include:

Oversight of High-Risk Processing Activities: If a System is used for commercial purposes and involves high-risk processing (as defined by the DIFC DP Law), the following primary' requirements apply:

- The AI system deployed by the DIFC entity **must be certified** under a relevant certification scheme established by the DIFC Commissioner.
- An **Autonomous Systems Officer ('ASO') must be appointed.** This is an individual who has the same or substantially similar competencies, status, role and task of a [Data Protection Officer (DPO)] as set out in Article 17 and Article 18 of the [DIFC DP] Law".

Accountability: Regulation 10 sets out the roles of Deployer, Operator and Provider.

- Deployer – directs or benefits from the operation of a System
- Operator – is itself a Provider that operates or supervises a System on behalf or otherwise for the benefit, and on the direction of a Deployer (regardless of whether or not it controls the processing of personal data in the System).
- Provider – develops or commissions the development of a System in order to sell it to Operators or Deployers.

It further clarifies that a Deployer is akin to a Controller under the DIFC DP Law and an Operator is akin to a Processor.

Please note, the System itself is certified, not the DIFC entity. As such, pursuant to 10.3.3 any DIFC entity regardless of status is obligated to ensure that any System it deploys or operates is certified.

Finally, as stated in Regulation 10.3.3(d), both a Deployer or Operator must appoint an ASO.

Example:

Certification - A local DIFC entity uses a System provided by a Provider either within its own organisation as a part of intracompany / shared services, or by a third party Provider, for commercial purposes.

- If the DIFC entity is the Deployer, and the System has not been previously certified, then it must certify the System before deploying for commercial purposes

- If the DIFC entity is the Operator, and the System has not been previously certified, then it must certify the System before operating for commercial purposes

ASO - If the local DIFC entity, regardless of status as Deployer or Operator, on its own or part of the wider group, processes personal data in a high risk manner, a DPO should have already been appointed and, if caught by Regulation 10, would ordinarily appoint an ASO as well. The DPO and the ASO may be the same individual, if the DIFC entity so chooses.

Certification Requirements:

Sample certification frameworks outlining the requirements and procedures for obtaining certification of a System is posted on the DIFC website sub-menu on Regulation 10. Certifications will be assessed and granted by Accreditation Certification Bodies, which are appointed by the DIFC Data Protection Commissioner. Guidance on the above points is also available on the DIFC website.

SUPPORTING YOUR ORGANISATION

As ever the Commissioner's Office aims to support businesses subject to the Data Protection Law and Regulations where new and additional requirements are established. As such, your organisation may benefit from:

Training and Outreach – There will be opportunities to learn more about Regulation 10, engage in workshops to assist with assessing the privacy by design and other requirements, and updates about how to manage any certification obligations.

Guidance -

- DIFC DP Regulation here
- Regulation 10 FAQs here
- Guidance here
- Accreditation and Certification Framework here