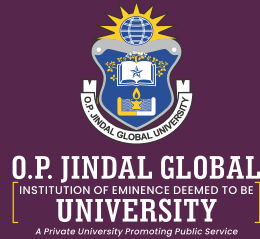


Comments on _____ Proposal relating to Amendment to Data Protection Regulations Dubai International Financial Centre (DIFC) Authority

18 July 2026





A About the Cyril Shroff Centre for AI, Law & Regulation

The Cyril Shroff Centre for AI, Law & Regulation (the “CSCAILR”) is a leading hub and centre of excellence that strives to produce high-quality research and actionable policy recommendations. We engage directly with policymakers and connect academic scholarship with policy implementation with the objective of enabling India to develop state-of-the-art frameworks for the regulation and governance of AI.

CSCAILR is a pioneering initiative at Jindal Global Law School (JGLS), O.P. Jindal Global University (JGU), India's top-ranked and globally reputed law school. Built under a generous endowment by Mr. Cyril Shroff, one of India's leading lawyers, CSCAILR is uniquely positioned to partner with academics, policy makers, think-tanks, law firms, the judiciary and businesses, to produce insights tempered with multi-stakeholder viewpoints.

The Proposed Regulations will have direct consequences for entities in India and elsewhere in the Global South. Indian technology firms, global capability centres and system vendors engaged by DIFC-licensed entities will be subject this regime. In addition, as a research centre devoted to the legal and regulatory questions raised by artificial intelligence (AI), with a particular focus on how AI governance frameworks operate across jurisdictions, our interest is in the comparative significance of Regulation 10. The DIFC Authority has taken a position on the accountability of autonomous systems that few instruments have attempted, and the choices made here are likely to inform how the question is approached elsewhere, including in India.

Detailed Comments

The following comments have been made in response to the specific questions raised by the DIFC Authority.

Q.1 Do you understand and agree with the changes to Regulation 10, particularly with respect to the AI-native jurisdiction initiative? If not, please provide your reasoning and details of specific concerns.

1

Allocation of responsibility as between Providers, Deployers and Operators

We support the changes. But, we identify a structural concern arising from the placement of accountability for design. The design concepts in Regulation 10.3.1 are addressed to the System, and Regulation 10.3.2 prohibits any person from providing or offering a non-compliant System. However, the accountability architecture of Regulation 10 does not reach the Provider:

- The deeming provisions in Regulation 10.3.5 assign Controller status to the Deployer and Processor status to the Operator. The Provider, as defined in Regulation 10.1.1(d), is deemed nothing. Regulation 10.1.1(c) captures a Provider only where it operates or supervises the System on the Deployer's direction. A Provider that develops and licenses a System which the Deployer then operates itself falls outside the definition of Operator entirely. Where a Provider is an Operator, it is deemed a Processor, and Processor obligations concern processing on instruction rather than design integrity.
- As a result, the party controlling design, training and in-built safeguards sits outside the general requirements in Regulation 10.2.1, the transparency and evidentiary obligations in Regulation 10.2.2, and the Data Subject complaint route in Regulation 10.3.6.
- The guidance to Regulation 10.3.1 makes this a considered choice, anticipating that Deployers and Operators will "procure Systems only from 'developers' that can give them contractual comfort of compliance-by-design with these principles."

We recognise the jurisdictional logic: a Provider developing a System offshore may lack a DIFC nexus, whereas the Deployer operating it in the Centre does not. Accepting that constraint, we suggest DIFCA consider specifying a minimum contractual floor which can be undertaken through these regulations or any other supporting instrument. The contractual floor will simply be a set of rules specifying the matters on which a Deployer or Operator must obtain contractual assurance from a Provider before deployment. Regulation 10 presently relies on contractual privity to carry design accountability without prescribing what those contracts must contain, leaving the effectiveness of the mechanism to the bargaining position of the parties. A specified floor would preserve the current architecture while giving it determinate content.

Q.2 Do you understand and agree with new concept definition of “Safety” included in Regulation 10.3.1(f)? Please provide your reasoning and details of specific feedback, including any ambiguity or concerns.

2 The concept of Safety does not presently carry content distinct from the existing concepts

We support the inclusion of Safety as a sixth design concept but consider its formulation to require reconsideration. Its operative content, the prevention of discriminatory or biased outcomes through oversight, testing and controls, is already required by 'Fairness' under Regulation 10.3.1(b) and by the 'Ethical' concept under Regulation 10.3.1(a). Its remaining element, the assessment and mitigation of risks of harm, overlaps with Regulation 10.3.1(d).

It is submitted that the distinct work available to Safety is the regulation of harms arising from the operation of a System as such, as opposed to harms arising from unfair outcomes, which 'Fairness' governs, or from loss of confidentiality, which 'Secure' governs. These include psychological harm, behavioural manipulation, the engineering of dependence, and reasonably foreseeable misuse. They are of particular significance where a System interacts with individuals in a conversational or companion capacity, a category expressly contemplated by the guidance to Regulation 10.1, and they are not addressed elsewhere in the Regulations.

We accordingly recommend that Regulation 10.3.1(f) be redrafted along the following lines.

“Safety: a System must be designed, developed and operated with safeguards to identify the Personal Data that it Processes, and to assess, mitigate and monitor on an ongoing basis the risks of harm to individuals arising from its operation, including reputational, psychological, financial, professional and physical harm, harm arising from the manipulation of or undue influence upon a Data Subject's decision-making or behaviour, and harm arising from reasonably foreseeable misuse of the System.”



O.P. JINDAL GLOBAL
INSTITUTION OF EMINENCE DEEMED TO BE
UNIVERSITY
A Private University Promoting Public Service



CYRIL SHROFF
CENTRE FOR AI,
LAW & REGULATION
O.P. JINDAL GLOBAL UNIVERSITY



Jindal Global Law School
India's First Global Law School

 O.P. Jindal Global University, Sonipat Narela Road,
Sonipat-131001, (Delhi NCR), Haryana, India



jindalglobaluni



jindalglobaluni



jindalglobaluni



jindalglobaluni



jguvideo

JGU - An Initiative of Jindal Steel & Power Foundation



WWW.JGU.EDU.IN