PRACTITIONER PERSPECTIVE

Ksenia Andreeva

Morgan, Lewis & Bockius LLP

Ksenia Andreeva of Morgan, Lewis & Bockius LLP explains Saudi proposals on Global AI Hubs.

The Saudi Data and Artificial Intelligence Authority (SDAIA) has released a draft Global AI Hub Law. This is an ambitious legislative proposal designed to ensure Saudi Arabia maintains its role as one of the leaders in AI, the data economy and digital infrastructure. The draft law aims to establish an innovative legal framework which will attract global investment, foster cross-border collaboration, and enhance data security in Saudi. It is another step towards Saudi defining its own approach to data sovereignty and establishing a regional benchmark. SDAIA has been inviting feedback from local and international stakeholders via the Saudi government platform or directly to the Communications, Space and Technology Commission at AIHub@cst.gov.sa. At the heart of this proposal is the concept of 'AI Hubs', sovereign or semi-sovereign data centres (or isolated and clearly demarcated parts of these) located Saudi Arabia but which hold data that falls under the legal protections of a foreign country. Like traditional embassies, these data centres will have a special legal status, and will ensure data is governed under the jurisdiction of the data-owning country or entity. The draft law does not use the term 'AI' in the law's text other than in its title, and it seems the use of AI technology is not a prerequisite for a hub to fall under the regulations, although it is expected these data centres will use advanced technologies). The model suggested in the draft law is an important alternative to traditional data localisation approaches. Instead of mandating that data remain within its country of origin, which can often be financially and administratively burdensome, it enables companies to store data in Saudi Arabia with sovereign protections intact. This should appeal particularly to governments and global organisations seeking secure, neutral, and geopolitically stable environments for data hosting. The draft law only allows the Saudi Council of Ministers to intervene in the operations of the hubs in exceptional circumstances, where this is crucial to protect the Kingdom's safety, national security, and sovereignty. There are three types of hubs depending on the nature of the hosted data and protection level required. This should help the law flexibly address a range of scenarios, from public-interest research to highly sensitive governmental data storage. Each type has its own structure and operational requirements, many of which will be determined as work on the draft regulation progresses. Private hubs will be used for hosting data, apps, infrastructure and services by a foreign government with a bilateral agreement with Saudi Arabia (a Guest Country) for the sole use of the Guest Country. Here the laws and regulations applicable in the guest country apply. The Guest Country is responsible for ensuring the Hub complies with 'requirements of applicable international law', and has 'full responsibility for the same before the Kingdom and the international community'. The second type is the Extended Hub. These will involve data, apps, infrastructure and services hosted by a private data centre operator with an agreement with a Saudi regulator (Competent Authority) and in line with an arrangement between the Competent Authority and the Guest Country. Here the applicable law and regulations is also that of the Guest Country. Extended Hub operators have to meet specific requirements on cybersecurity, operational transparency, and dispute resolution mechanisms. The last type will be the virtual hub which will provide virtualized data hosting and management services to customers by a private Saudi-incorporated and authorised services provider. In this case the applicable laws and regulations will be those of the country where the Customers are domiciled (the Designated Foreign State). In this case content (i.e. any software, apps, data, text, audio, video, or images) a Customer or its end users store, transmit or process via a Virtual Hub) are protected under the laws of the Designated Foreign State, with the Saudi courts supporting the enforcement of respective court decisions. A Competent Authority, a central oversight body, responsible for issuing certifications, conducting audits, and mediating conflicts will also be created which could either be SDAIA or a separate new authority determined by the Council of Ministers. The Competent Authority will initiate negotiations with Guest Countries to support the establishment of private hubs. It will also maintain a register of information about all hubs, Guest Countries, operators and service providers, and associated agreements or bilateral agreements on the operations of the hubs. It is expected this register will be publicly available. The Competent Authority will also share information with Designated Foreign States as a part of their oversight of Virtual Hubs' service providers.

need to increasingly localise. Consumer and competition laws are being tightening and there are stricter rules on pricing, advertising, and distribution. There is an evolving regulatory framework which includes new environmental and sustainability regulations, targeting packaging and waste management, which have meant we must rethink product design and supply chains. The rapid rise of e-commerce has brought fresh rules around digital consumer rights. In FMCG, the pace is relentless as is the change. One of the biggest challenges is staying ahead of a fast-moving regulatory landscape while navigating different legal systems and business expectations across the region. Each market has its own complexities.

There is no playbook. We are constantly revising contracts, reworking consent mechanisms, tightening claim reviews, and adapting commercial terms. In markets with unclear or rapidly changing laws, you often have to find practical solutions that balance compliance with business continuity and speed. I have realised that, even in a leadership role, you do not always have all the answers. What makes a difference is being honest about the challenges, keeping lines of communication open, and creating space so the team feels safe to raise concerns and take ownership.