



keypoint

AI Flash

May 2026

GCC

Kingdom of Saudi Arabia (KSA)

SDAIA - Consultation period for draft responsible AI policy closes

On **3 May 2026**, public consultation on SDAIA's draft responsible AI policy closed. The draft applies to government bodies, the private sector, non-profit sector and individuals developing or using AI solutions in Saudi Arabia and includes requirements linked to governance, testing, data protection, cybersecurity, content moderation, non-discrimination, performance monitoring and registration.

Saudi Arabia appears to be converting responsible AI expectations into a more structured operating model. Organisations should not wait for final issuance before preparing AI inventories, risk classification, testing evidence, human oversight arrangements and monitoring controls.

Kingdom of Bahrain

With no new Bahrain-specific AI laws or policy updates identified for May 2026, organisations should continue to embed AI governance into procurement, vendor due diligence, privacy reviews, workforce training and business-as-usual controls, rather than treat AI as a separate innovation activity.

The United Arab Emirates

First cohort of government AI agents launched

In **May 2026**, the UAE government launched its first cohort of AI agents during the national Agentic AI Retreat in Abu Dhabi. The agents cover procurement, tax auditing, customer happiness and technical support and form part of the UAE's plan to transition 50% of federal government services and operations to AI-powered models within two years.

This marks a practical shift from AI strategy to AI execution in government operations. For organisations, the governance message is clear: agentic AI requires stronger controls around authority limits, audit trails, escalation, service quality, data protection and accountability, particularly where AI systems perform actions rather than merely provide recommendations.

Qatar

Shura Council committee continues AI governance review

On **3 May 2026**, the Health, Public Services and Environment Affairs Committee of Qatar's Shura Council discussed (and deferred) a request for a general debate on the regulation and governance of AI.

Organisations operating in Qatar should monitor the legislative process closely and begin preparing governance controls around privacy, accountability, ethical use and data management ahead of any formal AI framework.

Oman

AI special zone established

On **30 April 2026**, Oman issued Royal Decree 50/2026 establishing an AISZ in Muscat, with projects granted incentives, advantages, exemptions and facilities under Oman's special economic zones and free zones framework.

Oman is treating AI as an economic development and investment priority, not just as a governance issue. Companies exploring AI deployment in Oman should consider both compliance expectations and potential opportunities linked to AI infrastructure, R&D, localisation and investment incentives.

International European Union

Draft guidelines on high-risk AI systems and transparency obligations

On **19 May 2026**, the European Commission published draft guidelines on the [classification of high-risk AI systems](#) and on Article 50 transparency obligations and opened a [targeted public consultation](#). The draft transparency guidelines clarify obligations relating to AI systems that interact with individuals, AI-generated or manipulated content (including deepfakes), emotion recognition and biometric categorisation systems, while the high-risk AI guidance provides additional interpretation on Annex III classifications and risk determination.

The EU AI Act is now entering a practical implementation phase where organisations are expected to move beyond high-level awareness into operational compliance planning. Organisations should be actively assessing whether any systems fall within Annex III high-risk categories and whether Article 50 transparency obligations apply, prepare technical documentation and governance evidence, and monitor further developments regarding implementation timelines and supervisory expectations.

United States

NIST publishes AI agent security analysis

On **18 May 2026**, [NIST](#) published a [summary](#) of responses to its request for information on security considerations for AI agents, building on its wider work on AI agent standards and security. The work focuses on the specific risks that arise when AI model outputs are connected to software systems capable of taking action.

AI agents are becoming a separate security and governance category. Organisations deploying agentic AI should assess identity, authentication, authorisation, tool access, logging, abuse prevention and red-teaming as core controls, rather than relying only on traditional AI model risk assessments.

China

Consultation period for draft digital-human rules ends

The consultation period for China's draft regulations on digital humans and virtual human content closed on **6 May 2026**.

China is increasing regulatory scrutiny of emotionally-engaging, identity-based AI services. Businesses developing AI companions, virtual influencers, avatars or human-like customer-service agents should pay close attention to themes including consent, minors, addictive design, identity misuse, labelling and public-order risks.

Contact Keypoint's technology consulting team

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com

Darrshan Manukulasooriya
Executive Manager
d.manukulasooriya@keypoint.com

Sagar Rao
Senior Manager
sagar.rao@keypoint.com

Mahesh Girish
Senior Consultant
mahesh.girish@keypoint.com

Talal Alqahtani
Assistant Consultant
talal.alqahtani@keypoint.com