

AI and data rules in the Gulf and Egypt, 2026

What applies to an AI system that processes personal data, country by country. A one-page checklist.

Updated: 25 October 2026

Country	Data law and status	Can personal data leave?	Where it tightens	AI-specific rules
Saudi Arabia	PDPL, fully enforced since 14 Sep 2024 by SDAIA. Fines up to SAR 5 million per violation; 48 decisions in 2025.	Yes, with safeguards (standard clauses, binding rules or a certificate) and a risk assessment. A draft of 6 Oct 2026 would add in-Kingdom storage (comments until 5 Nov).	Government and critical infrastructure: NCA controls are mandatory; classified government data stays on government cloud. Banks: SAMA no-objection for material outsourcing.	No AI law. SDAIA ethics principles and AI risk framework are guidance; a Responsible AI Policy and NCA AI guidelines are in draft.
UAE	Federal Decree-Law No. 45 of 2021; implementing regulations not issued as of June 2026.	No blanket localisation; the transfer mechanics wait on the regulations.	DIFC Regulation 10 has covered AI and autonomous systems since September 2023.	A Federal Authority for AI and Data, announced 14 June 2026, reporting to the Cabinet.
Egypt	Law No. 151 of 2020; executive regulations Nov 2025; compliance due from 1 Nov 2026. Controllers and processors need a licence.	Only with a licence or permit, and only to the countries named in it, cloud included.	Breaches: the Center within 72 hours, then affected people within three business days.	National AI Governance Framework (Mar 2026): four risk tiers, LLM transparency, lightweight models preferred.
Qatar	Law No. 13 of 2016 on personal data privacy.	Yes: controllers may not restrict transfers except in defined cases (Article 15).	Special-nature data (health, children, criminal records and more) needs prior permission (Article 16). QFC has its own regulations; QCB issued AI guidelines for banks (Sep 2024).	No AI law; NCSA guidelines expect auditability, traceability and documentation.
Kuwait	No general data protection law. CITRA Regulation No. 26 of 2024, whose scope sources dispute.	Users must be told about transfers; CITRA approval may be needed. Sources disagree on approval for sensitive data.	The old classification policy (Tier 3/4 data in Kuwait) was repealed in Feb 2024. Breaches reported within 24 hours.	No AI framework yet. CITRA roadmap: new localisation rules for 5G-Advanced (Q4 2026), a telecoms AI policy (2027).
Oman	PDPL (Royal Decree 6/2022), fully enforced since 5 Feb 2026; amended by Royal Decree 68/2026.	No general localisation; sources read the transfer conditions differently.	TRA cloud rules: Level 3 and 4 data (state, financial, health, energy) needs prior approval to leave Oman.	Right to object to automated decisions, with human review (Sep 2026). National AI policy (May 2025).
Bahrain	PDPL No. 30 of 2018.	Only to countries on the Authority's list (83 per DLA Piper) or with case-by-case authorisation.	Article 15: automated processing of sensitive data, and biometrics, need authorisation. Breaches within 72 hours.	National AI policy (Jul 2025). The AI bill is still a proposal.

Five checks before any AI deployment

1. Where does each layer run: the model, retrieval, safety, logs?
2. Which of your data is sensitive, classified or regulated by sector?
3. Does any part of the system send data abroad, even for licensing or telemetry?
4. Can you meet the breach clock: 24 hours in Kuwait, 72 hours in Saudi Arabia, Egypt and Bahrain?
5. Can you show who asked, what the system saw and what it did?

A summary of public sources, not legal advice. Check the official texts and your legal counsel before acting. Sources and detail for each country: nooraisolutions.com/en/blog/

NoorAI · On-premises Arabic AI · contact@nooraisolutions.com