Quels pays du Golfe disposent de lois sur la protection des données, et en quoi diffèrent-elles ?

Réponse courte : Cinq des six États du CCG disposent désormais de lois complètes sur la protection des données — l'Arabie saoudite, les Émirats arabes unis, Bahreïn, le Qatar et Oman. Le Koweït fait exception, adoptant à la place une approche sectorielle. Elles diffèrent principalement sur la rigueur du consentement, la préférence en matière de localisation, et le mécanisme de transfert.

Le tableau régional

Juridiction	Statut	Caractéristique distinctive
Arabie saoudite	PDPL en vigueur (pleinement effective depuis septembre 2024)	Préférence de localisation la plus forte ; SCC approuvées par la SDAIA
Émirats arabes unis	Décret-loi fédéral 45/2021	Bases légales de type RGPD ; le DIFC et l'ADGM appliquent des régimes distincts
Bahreïn	En vigueur depuis 2019	Fortement inspiré du RGPD ; portée extraterritoriale ; application mature
Qatar	En vigueur depuis 2017	Le plus ancien de la région ; davantage centré sur le consentement
Oman	Pleinement effectif le **5 février 2026**	Reflète les principes du RGPD ; fin de la période de grâce
Koweït	Pas de loi complète	Uniquement sectoriel — réglementation du CITRA pour les télécommunications et les technologies de l'information

Statut au moment de la rédaction ; à confirmer auprès d'un conseil juridique local.

L'axe le plus déterminant

Deux variables distinguent ces régimes en pratique :

- **Rigueur du consentement.** Le Qatar et l'Arabie saoudite privilégient une approche centrée sur le consentement. Les Émirats arabes unis autorisent un ensemble plus large de bases légales, se rapprochant du RGPD.
- **Préférence en matière de localisation.** L'Arabie saoudite est la plus stricte ; les Émirats arabes unis et le Qatar adoptent une approche davantage fondée sur le risque et axée sur les garanties.

Pourquoi une seule architecture répond aux six régimes

Ces régimes divergent sur le mécanisme mais convergent sur le fond : collecter le minimum, le sécuriser, et contrôler sa destination.

Étant donné que Cyber Crucible ne collecte jamais de clés, d'identifiants, de jetons ou de contenu, et peut fonctionner en environnement isolé (air-gapped) avec une télémétrie sortante nulle, la réponse à la question « quelles données personnelles ce fournisseur détient-il, et où vont-elles ? » est brève dans chacun de ces régimes. Répondre aux exigences les plus strictes — celles de l'Arabie saoudite — couvre le reste.

Oman constitue la priorité à court terme pour quiconque n'a pas encore examiné son infrastructure, compte tenu de l'échéance de février 2026.

> Le détail par pays figure dans les **Guides de conformité par pays**.

Revision #1
Created 2026-07-24 07:05:59 UTC by Dennis Underwood
Updated 2026-07-24 07:05:59 UTC by Dennis Underwood