

AI, TECHNOLOGY & DIGITAL ASSETS · 10 JULY 2026 · 10 MIN READ

AI and Personal Data in the UAE: Lawful Design, Vendors and Automated Decisions

UAE businesses need to map AI data flows, establish lawful purpose, manage vendors and build meaningful review into automated decisions before deployment.

Akash Chetwani, CFA
SENIOR PARTNER · ADVISORY

IRAA Global Advisory

Contents

AI, TECHNOLOGY & DIGITAL ASSETS · 10 MINUTE READ · JULY 2026

UAE businesses need to map AI data flows, establish lawful purpose, manage vendors and build meaningful review into automated decisions before deployment.

-
- | | |
|----|----------------------------------|
| 01 | Questions for every AI data flow |
|----|----------------------------------|
-
- | | |
|----|--------------------------------|
| 02 | Map data beyond the prompt box |
|----|--------------------------------|
-
- | | |
|----|---|
| 03 | Establish purpose and lawful processing |
|----|---|
-
- | | |
|----|---|
| 04 | Assess high-risk processing before launch |
|----|---|
-
- | | |
|----|---|
| 05 | Control automated decisions and profiling |
|----|---|
-
- | | |
|----|--------------------------------------|
| 06 | Contract for the real vendor service |
|----|--------------------------------------|
-
- | | |
|----|---------------------------------------|
| 07 | Secure the model and its integrations |
|----|---------------------------------------|
-
- | | |
|----|--------------------------------|
| 08 | A privacy-ready AI launch gate |
|----|--------------------------------|
-
- | | |
|----|---|
| 09 | Design rights handling before requests arrive |
|----|---|
-
- | | |
|----|---|
| 10 | Manage international and group data flows |
|----|---|
-
- | | |
|----|------------------|
| 11 | Official sources |
|----|------------------|
-

An AI project that uses personal data is a data-processing system before it is an innovation project. UAE businesses should establish purpose, lawful grounds, transparency, security and individual rights before data is sent to a model.

Federal Decree-Law No. 45 of 2021 governs personal-data processing within its scope and contains requirements for controllers and processors, data-subject rights, cross-border processing and impact assessment. Sector and free-zone regimes may also apply, so the first task is to identify jurisdiction.

Questions for every AI data flow

WHAT DATA?	Identify personal, sensitive, biometric, source and inferred data.
WHY?	Define the specific purpose and applicable legal basis.
WHO?	Map controller, processor, vendor, recipient and human decision-maker.
WHERE?	Record storage, model processing, support access and cross-border transfers.
HOW LONG?	Set retention for inputs, prompts, outputs, logs and training copies.

Map data beyond the prompt box

AI systems create more data than users submit. A service may store prompts, uploaded files, embeddings, model outputs, feedback, logs, account identifiers and security telemetry. Outputs can infer characteristics not present in the original dataset.

Draw the flow from collection to deletion. Include source systems, integration layers, cloud regions, sub-processors, support teams, training options, backups and exports. Verify the map against technical configuration and contract terms.

Classify sensitive data and establish whether the use case can operate with anonymised, pseudonymised or synthetic information. Data minimisation reduces privacy, security and model-governance risk.

Establish purpose and lawful processing

Consent is not the only possible basis, and it is not automatically valid because a privacy notice mentions AI. The law sets conditions and exceptions that must be analysed for the specific processing. Document the purpose, necessity and applicable basis before collection or reuse.

Training a model, generating a recommendation and monitoring employees can be distinct purposes. Data collected to deliver a service should not be reused for unrelated model training without analysis. Vendor product improvement is also a separate use that must be understood.

Privacy information should explain material processing in clear language: data types, purpose, sharing, retention, transfers, rights and automated decisions where relevant. Avoid claiming a system is fully automated if employees routinely intervene, or human-led if reviewers merely accept its output.

Assess high-risk processing before launch

The UAE PDPL requires an impact assessment in specified high-risk circumstances, including processing involving modern technologies that may pose a high risk to privacy and confidentiality. An AI impact assessment should combine privacy, fairness, security and operational analysis.

Describe individuals affected, data, purpose, necessity, proportionality, risks and safeguards. Evaluate incorrect decisions, exclusion, discrimination, sensitive inference, re-identification, surveillance, leakage and inability to exercise rights.

The assessment should drive design. Reduce fields, add human review, shorten retention, improve explanation, restrict model use or decide not to proceed. Approval without design change is not a meaningful assessment.

“Privacy by design means changing the system before launch, not explaining the risk after deployment.”

Control automated decisions and profiling

Article 13 gives data subjects a right to information including decisions made through automated processing and profiling. Businesses should know which systems make or materially influence decisions and be able to explain the relevant process.

Maintain decision logs sufficient to identify input version, model version, output, human review and outcome. Provide correction and escalation paths when data is inaccurate or the recommendation is disputed.

Test outcomes across relevant groups and conditions. A model can reproduce historical bias or create proxy discrimination even if protected characteristics are removed. Document thresholds and false-positive consequences.

Contract for the real vendor service

Review whether the provider acts as processor, independent controller or both for different activities. The contract should address instructions, confidentiality, security, sub-processors, locations, breach support, deletion, audit evidence, model training and assistance with rights.

Check product settings. A contract may promise no training only when an administrator disables a feature or uses an enterprise tier. Preserve configuration evidence and monitor vendor changes.

Plan exit and portability. The company should be able to export required records, delete data and replace the service without losing control of a regulated business process.

Secure the model and its integrations

Use role-based access, multifactor authentication, encryption, secrets management and logging. Separate development and production, limit privileged access and test prompt injection, data exfiltration and unsafe tool actions.

Connect breach response to privacy assessment. Determine affected data, people, locations, consequences, containment and notification obligations. Preserve evidence without retaining personal data indefinitely.

A privacy-ready AI launch gate

01	Map: Trace inputs, inferences, outputs, logs and transfers.
02	Justify: Record purpose, necessity and legal basis.
03	Assess: Complete impact review before high-risk processing.
04	Explain: Provide notices and automated-decision information.
05	Contract: Control vendors, training, sub-processors and exit.
06	Operate: Monitor rights, incidents, drift and material changes.

AI privacy compliance is strongest when it is embedded in product decisions. A system that uses less data, explains its role, supports correction and limits vendor reuse is easier to defend and more likely to earn customer and employee trust.

Design rights handling before requests arrive

Businesses should decide how a person can access, correct or challenge information connected to an AI service before launch. That requires more than a generic privacy inbox. The team must know where prompts, source documents, embeddings, model outputs, feedback and audit logs are stored; which records can be retrieved by person; and which vendor must assist. Retention rules should distinguish operational evidence from unnecessary histories that increase exposure without improving the service.

Not every output is a fact about a person, but an inference used to evaluate or treat someone may still be consequential. Product and legal teams should document how inaccurate inputs and outputs can be corrected, whether the original decision can be revisited and how a meaningful human reviewer receives the context needed to disagree with the system. A nominal approval click is not meaningful oversight if the reviewer lacks time, authority or an alternative source of evidence.

Manage international and group data flows

Many AI services involve data moving between a UAE customer, a regional operating company, a global group platform and several technical providers. Map those transfers and confirm the safeguards that apply rather than assuming a familiar vendor makes the flow acceptable. Contracts should identify processing locations, sub-processors, security responsibilities, deletion procedures and assistance with data-subject requests. The operating record should match the agreement; an unused contractual control provides little protection.

Finally, treat model and feature changes as privacy events. A provider may introduce new logging, training, retrieval or analytics functions under an existing product name. Change monitoring should trigger a fresh assessment when the purpose, data categories, recipients, retention, automation or risk to individuals materially changes. This discipline helps the business demonstrate that its stated purpose and safeguards remain true throughout the service lifecycle, not merely on the date the contract was signed.

Official sources

1. **Federal Decree-Law No. 45 of 2021 on Personal Data Protection**
2. **UAE AI Ethics Principles and Guidelines**
3. **UAE National Cloud Security Policy**

Online edition: <https://iraaglobal.com/insights/uae-ai-personal-data-lawful-design-vendor-automated-decisions/>



Akash Chetwani, CFA

SENIOR PARTNER · ADVISORY

Cross-border advisory for professionals, founders, investors, and globally connected families.

PHONE

+971 56 921 0222

EMAIL

info@iraaglobal.com

PROFILES

[LinkedIn](#) · [Contributor page and articles](#)

A connected advisory firm for businesses operating across borders.

OUR EXPERTISE

Audit & Assurance

Corporate Tax & VAT

Accounting & Bookkeeping

Finance & CFO Advisory

AML, Risk & Compliance

Business Advisory & Setup

Human Resources Advisory

AI, Technology & Digital Assets

India-UAE Cross-Border Advisory

Private & Family Advisory

Insight beyond numbers.

IRAA Global Advisory

503 Mustafawi Carpet Building, Sharaf DG Metro Exit 1
Dubai, United Arab Emirates

+971 56 921 0222 · +971 50 677 9455
info@iraaglobal.com · www.iraaglobal.com