LAW, RISK & COMPLIANCE · 24 JULY 2026 · 11 MIN READ

UAE Data Protection for Businesses: Consent, Vendors, Breaches and Cross-Border Processing

Data protection is an operating model for how personal information is collected, used, shared, secured and deleted. Contracts and privacy notices matter, but systems and daily decisions must support them.

Akash Chetwani, CFA
SENIOR PARTNER · ADVISORY

IRAA Global Advisory

EDITORIAL GUIDE

Contents

LAW, RISK & COMPLIANCE · 11 MINUTE READ · JULY 2026

Data protection is an operating model for how personal information is collected, used, shared, secured and deleted. Contracts and privacy notices matter, but systems and daily decisions must support them.

> The UAE’s federal Personal Data Protection Law turns privacy into an operating responsibility. A business must understand what personal data it controls, why it processes it, who receives it, how long it is retained and what happens when a customer, employee or regulator asks for an answer.

Federal Decree-Law No. 45 of 2021 applies to processing within its stated scope and includes obligations for controllers and processors, rights for data subjects, rules for cross-border processing and breach response. It also contains exclusions, while financial free zones and sector-specific laws may operate under distinct regimes. A company should therefore establish which legal framework applies to each activity before copying a generic global privacy policy.

Key data protection concepts

CONTROLLER	The person or establishment that determines the purpose and means of processing personal data.
PROCESSOR	A person or establishment that processes personal data for the controller under its supervision and instructions.
CONSENT	Where relied upon, consent must indicate specific, clear and unambiguous acceptance through a clear positive statement or action.
SECURITY	Controllers must apply appropriate technical and organisational measures considering the nature, scope, purpose and risks of processing.

Map the data before writing the policy

Most businesses hold more personal data than their privacy notice suggests. Customer records sit in the CRM, finance platform, email, messaging tools, website analytics, call recordings, support tickets and archived spreadsheets. Employee data may sit with HR, payroll, insurers, immigration agents, background-screening providers and group companies.

Create a processing inventory that records the data subject, data elements, purpose, legal basis, source, users, recipient, system, storage location, retention period, security classification and transfer destination. Include biometric, health and financial information where relevant because the consequences of misuse can be greater.

The inventory is not a one-time exercise. Procurement should not activate a new cloud tool until the data flow is recorded and approved. Marketing should not add a new audience or tracking technology without assessing the changed purpose. HR should update the map when onboarding or benefit processes change.

Choose a lawful processing basis, not a convenient label

Consent is important but it is not the only circumstance in which the Law permits processing. Article 4 lists cases in which personal data may be processed without consent, including circumstances connected with contracts, legal obligations, protection of interests and other defined grounds. The correct basis depends on the purpose and facts.

If consent is used, the request should be specific, clear and separate from unnecessary terms. Pre-ticked boxes, inactivity or bundled acceptance can undermine evidence that a clear positive action occurred. The business should retain when, how and for what the individual consented, and offer a practical way to withdraw where applicable.

A purpose stated broadly as “business use” is unlikely to guide decisions. Describe why the information is necessary: deliver a contracted service, process payroll, verify identity, meet a legal duty, respond to an enquiry or send a particular form of marketing. If a new use is materially different, reassess it before reuse.

> *“A privacy notice should describe the business that actually exists—not the business imagined when the template was downloaded.”*

Give people meaningful information

Article 13 gives data subjects a right to information including the types of data processed, purposes, automated decisions, recipients inside and outside the UAE, retention standards, rights procedures, cross-border safeguards, breach actions and how to complain. Before processing starts, the controller must provide specified information about purposes, sharing and cross-border protection.

Notices should be layered and accessible at the point of collection. A website notice alone may not cover CCTV, recruitment, events, recorded calls or offline forms. Use concise first-layer explanations with a link or route to complete information. Avoid legal jargon that hides important consequences.

Prepare a request procedure for access-related information, correction, erasure, restriction, objection and portability where applicable. The procedure should verify identity without collecting excessive new data, locate records across systems, protect third-party information and document any lawful refusal.

Control vendors as processors

Outsourcing a system does not outsource accountability. Before appointing a processor, assess security, location, subcontractors, incident history, deletion, business continuity and the ability to support data-subject requests. The contract should define instructions, confidentiality, permitted uses, access control, breach notification, audit information, subcontracting, return or deletion and transfer arrangements.

The commercial owner should understand the service, while legal, technology and privacy teams review risk. A low-cost application can create high exposure if it copies customer or employee information into an unmanaged environment. Maintain a vendor register and reassess critical processors after material changes.

Access should follow least privilege. Remove departed users promptly, review administrator accounts and separate production data from testing. If a vendor needs sample information for support, use masked or synthetic data where feasible rather than exporting the full live database.

Assess cross-border processing

Cloud hosting, regional support and group reporting can move or make personal data accessible outside the UAE. Articles 22 and 23 address cross-border processing. Management should identify the destination, recipient, transfer mechanism and protection measures rather than assuming that a global vendor’s standard contract resolves the issue.

Map remote access as well as physical storage. A database hosted in the UAE may still be accessed by an overseas support team. Conversely, data stored abroad may be protected through an applicable mechanism if the legal requirements are met. Record the analysis and ensure the privacy notice describes relevant sharing.

Prepare for a breach before it happens

A data breach includes unauthorised or unlawful access, copying, transmission, disclosure, destruction or alteration. Article 9 requires a controller that becomes aware of a breach prejudicing privacy, confidentiality or security to notify the UAE Data Office under the periods, measures and requirements set by the Executive Regulations. The notification content includes the nature and cause, approximate persons and records, DPO details, likely effects and corrective action.

The controller must also notify affected data subjects where the breach would prejudice their privacy and confidentiality, under the applicable requirements. A processor must notify the controller as soon as it becomes aware. Vendor contracts should therefore require fast escalation; a deadline beginning only after the vendor completes its investigation may leave the controller unable to act.

An incident plan should identify the decision team, evidence preservation, containment authority, legal assessment, regulator contact, customer communication and recovery steps. Run a tabletop exercise using a realistic scenario such as a compromised mailbox, misdirected payroll file or exposed CRM credential.

Retain only what the business can justify

The Law provides that personal data should not be kept after the processing purpose is exhausted, subject to permitted anonymisation and other legal needs. A retention schedule should reconcile privacy with tax, employment, corporate, litigation and sector rules. “Keep everything” is not a neutral position; it expands the impact of a breach and makes requests harder to manage.

01	**Inventory:** Map personal data across customers, staff, systems, vendors and locations.
02	**Purpose:** Record a specific purpose and lawful processing basis for each activity.
03	**Inform:** Place accurate, layered notices where collection occurs.
04	**Contract:** Control processors, subcontractors, access, incidents and deletion.
05	**Respond:** Establish data-subject and breach procedures with accountable owners.
06	**Delete:** Apply a defensible retention schedule and verify disposal.

Effective data protection gives management a reliable answer to three questions: what information do we have, why do we have it and who can use it? When those answers are embedded in procurement, marketing, HR, IT and incident response, privacy becomes part of controlled growth rather than an obstacle raised after a project has launched.

Official sources

1. **Federal Decree-Law No. 45 of 2021 Concerning Personal Data Protection**
2. **Federal Decree-Law No. 44 of 2021 Establishing the UAE Data Office**

Online edition: **https://iraaglobal.com/insights/uae-data-protection-business-consent-vendors-breaches/**

ABOUT THE CONTRIBUTOR

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**

IRAA GLOBAL
AUDIT · TAX · ADVISORY

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

IRAA GLOBAL

AUDIT · TAX · 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

LAYOUT & DESIGN BY SURESH TAMANG