

CRAVO ECOSYSTEM

Comprehensive Privacy Policy & Personal Data Protection Framework

Official Portal: cravonow.ae	Platform Version: 1.0.0 (Web & App)	Effective Date: August 4, 2026
Jurisdiction: Dubai, UAE	Statutory Compliance: UAE PDPL (Decree 45/2021)	Operating Entity: Cravo Technologies L.L.C.

STATUTORY PRIVACY COMMITMENT

Cravo Technologies L.L.C. ("Cravo", "We", "Us", "Our") is dedicated to protecting your personal data privacy and ensuring transparent data governance across **cravonow.ae**. This Privacy Policy outlines how personal data is collected, processed, secured, and retained across our multi-sided web platform, backend API servers, and AI recommendation engines in strict compliance with United Arab Emirates Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL).

1. STATUTORY COMPLIANCE BASIS (UAE PDPL)

This Privacy Policy is established pursuant to UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection ("PDPL"). Cravo Technologies L.L.C. operates as the Data Controller and Processor for personal data collected through its customer web portal, restaurant dashboards, driver applications, and system administration consoles.

2. CATEGORIES OF PERSONAL DATA COLLECTED

Cravo collects and processes specific personal and technical data categories necessary to deliver hyper-personalized food delivery and dietary management services:

Data Category	Data Attributes Collected	Primary Operational Purpose & Function
Identity & Profile Data	First Name, Last Name, Email Address, Phone Number, Password Hash (bcrypt), User Role.	User registration, JWT authentication, role-based authorization, and account management.
Biometric & Health Telemetry	Daily step count, active calories burned, daily energy expenditure, FitnessConnected status flag.	Calculates daily available calorie balance via Google Fit / Health Connect API. Collected ONLY upon explicit user opt-in.
Financial & Budget Data	Monthly budget limit (MonthlyBudget), cumulative monthly spend, transaction IDs, Stripe payment tokens.	Enforces monthly budget spending controls and executes secure payment processing via Stripe. Raw card details are NEVER stored.
AI Interaction & Mood Data	Free-text mood prompts (MoodText), AI chat history (chatWithAI), food preferences, interaction logs.	Powers AI meal recommendation engine and personalized discount generation algorithms.
Geospatial & Telemetry Data	Delivery address text, GPS coordinates (latitude/longitude), real-time courier location updates.	Live order delivery tracking, route optimization via Google Maps API, and courier dispatches.
Technical & System Logs	IP address, browser/device parameters, stateless JWT access tokens, system performance logs.	Ensures platform security, API token verification, fraud detection, and system health monitoring.

3. LAWFUL PURPOSES OF DATA PROCESSING

Cravo processes your personal data strictly for the following lawful operational objectives:

- **Order Fulfillment & Dispatch:** Transmitting order selections to Restaurant Partners and routing spatial delivery coordinates to assigned Delivery Couriers.
- **AI Hyper-Personalization:** Analyzing culinary preferences, historical purchases, remaining daily calories, and monthly budget limits to generate tailored meal options.
- **Health Metric Synchronization:** Dynamically adjusting daily caloric allowances in real time based on fitness burn metrics pulled from authorized fitness frameworks.
- **Financial Management & Budget Tracking:** Enforcing user-configured spending warnings prior to checkout.
- **Security & Administrative Governance:** Authenticating JWT sessions, preventing fraudulent payment transactions, and facilitating system monitoring.

AI DATA PROTECTION & ZERO PUBLIC MODEL TRAINING GUARANTEE

Text prompts submitted to the Cravo AI Assistant and dietary parameters are processed via encrypted TLS 1.3 connections to our LLM infrastructure (OpenAI API). Personal identifying information (such as your legal name, phone number, or payment token strings) is NEVER sent to external LLM providers or sold to third-party data brokers. User prompts are NEVER utilized to train public foundational AI models.

4. FITNESS API INTEGRATION & GRANULAR CONSENT CONTROLS

4.1 Opt-in Framework: Health and fitness telemetry synchronization (Google Fit / Apple Health) operates strictly on an opt-in basis (`FitnessConnected == TRUE`). The system will never access health metrics without explicit user consent.

4.2 Immediate Revocation: Users maintain the right to disconnect fitness API integration at any time through Profile Settings by setting `FitnessConnected = FALSE`. Disconnection immediately halts all health data ingestion.

5. DATA SHARING & THIRD-PARTY INFRASTRUCTURE TRANSFERS

Cravo does NOT sell, rent, or monetize your personal data to third-party advertisers. Personal data is shared strictly with essential operational infrastructure providers:

- **Restaurant Partners:** Receive item details, food preference tags, and dietary notes necessary to prepare your meal.
- **Delivery Couriers:** Receive pickup/drop-off customer names, delivery address text, phone contact, and GPS coordinates during active dispatches.
- **Stripe API Gateway:** Receives tokenized payment details to charge credit cards securely without exposing raw card numbers to local servers.
- **OpenAI API (AI Infrastructure):** Receives pseudonymized text prompts and candidate menu parameters to execute natural language recommendations.
- **Google Maps Platform API:** Receives spatial coordinates to calculate delivery routes, distance metrics, and live map tracking overlays.

6. DATA STORAGE, SECURITY & ENCRYPTION PROTOCOLS

6.1 Centralized MySQL Infrastructure: All relational platform data is stored in centralized MySQL database instances hosted on cloud Virtual Private Servers (VPS).

6.2 Security Safeguards:

- **Transit Encryption:** All data transmitted between clients and backend APIs is encrypted using HTTPS / TLS 1.3 protocols.
- **Password Cryptography:** Passwords are hashed using `bcrypt` with strong salt factors prior to storage.
- **Session Security:** Authentication relies on signed, stateless JWT access tokens with strict expiration timeouts.

7. USER DATA RIGHTS UNDER UAE PDPL

In accordance with UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection, users possess the following statutory rights:

YOUR STATUTORY RIGHTS UNDER UAE LAW (DECREE 45/2021)

- **Right to Access & Export:** You have the right to request a digital copy of all personal records, order histories, and AI recommendation logs stored in our database.
- **Right to Rectification:** You may update profile details, budget constraints, and account credentials at any time via Profile Settings.
- **Right to Revoke Consent:** You may revoke permission for fitness telemetry processing at any time.
- **Right to Erasure ("Right to be Forgotten"):** You may request full account deletion. Upon verification, Cravo will purge your personal identification records, subject to statutory accounting and legal audit retention obligations.

8. CHILDREN'S DATA PROTECTION POLICY

Cravo is strictly intended for use by individuals who are at least 18 years of age. We do not knowingly collect or solicit personal data from minors. If we discover that an individual under 18 has created an account without verified parental consent, we will immediately purge all associated account records.

9. POLICY AMENDMENTS & NOTIFICATIONS

Cravo reserves the right to update this Privacy Policy at any time to reflect software updates, architectural changes, or statutory amendments. Material modifications will be communicated via in-app notifications or email alerts. Continued platform access after updates constitutes acceptance of revised terms.

CRAVO DATA PROTECTION & PRIVACY CONTACT:

Privacy Team: privacy@cravonow.ae | Legal Inquiries: legal@cravonow.ae
Operating Entity: Cravo Technologies L.L.C. | Dubai, United Arab Emirates
Official Privacy Portal: <https://cravonow.ae/privacy>