

FITKOBRA AI TECHNOLOGIES

Global Statutory Compliance, Data Protection, Regulatory Defense & Master Liability Shield

Application Identifier: com.fitkobra.app (Android & iOS) | Web Domain: www.fitkobra.com

Version: 2.4.0 (2026 Statutory Consolidation) | Classification: Public Legal & Regulatory Charter

1. EXECUTIVE PREAMBLE & SCOPE OF PROTECTION

This legal instrument constitutes the definitive, binding Global Compliance Charter, Privacy Policy, Data Safety Disclosure, and Non-Medical Liability Limitation for **FitKobra Technologies** ("FitKobra", "Company", "we", "us", or "our"). This document establishes an ironclad legal and technical architecture designed to eliminate regulatory exposure, protect the Company and its executive officers from civil penalties and statutory administrative fines, and satisfy the mandatory regulatory frameworks of all jurisdictions where the FitKobra mobile application and web portal are distributed, including:

- **Republic of India:** Digital Personal Data Protection Act, 2023 (DPDP Act 2023) and Rules enacted thereunder.
- **European Union & European Economic Area:** Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).
- **United Kingdom:** Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).
- **United States of America:** California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (CCPA / CPRA; Cal. Civ. Code § 1798.100 et seq.), US State Comprehensive Privacy Laws (Virginia VCDPA, Colorado CPA, Connecticut CTDPA, Utah UCPA, Texas TDPSA, Florida, Oregon), Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§ 6501–6506), and Federal Trade Commission Act (15 U.S.C. § 45).
- **Health Product & Clinical Software Regulators:** US Food and Drug Administration (FDA) Guidance on Policy for Device Software Functions and Mobile Medical Applications, and EU Medical Device Regulation (EU MDR 2017/745).
- **Global Mobile App Store Ecosystems:** Google Play Developer Program Policies (specifically Health Connect Policy, User Data Policy, In-App and Web Account Deletion Mandates, and Ads Policies) and Apple App Store Review Guidelines (specifically Guidelines 5.1.1, 5.1.2, 5.1.3, and App Tracking Transparency).

2. STATUTORY REGULATORY FINES & COMPLETE LEGAL SHIELD

Modern data privacy statutes impose staggering administrative fines for failure to protect data, unauthorized processing, lack of lawful basis, failure to honor erasure requests, or unlawful processing of minor data. FitKobra's technical architecture and policy declarations are calibrated to completely neutralize liability under each statutory penalty regime:

STATUTE / JURISDICTION	MAXIMUM STATUTORY FINE / PENALTY	TRIGGERING RISK AREA	FITKOBRA ENFORCED IMMUNITY MECHANISM
India DPDP Act 2023 (Schedule)	₹250 Crores (~\$30,000,000 USD) per occurrence for failure to take reasonable security safeguards.	Data breach, insecure database storage, credential leak, lack of TLS encryption.	Cloud Firestore client-side security rules, AES-256 cloud encryption at rest, TLS 1.3 in transit, strict principle of least privilege, zero public database endpoints.
India DPDP Act 2023 (Sec 9 & Sched)	₹200 Crores (~\$24,000,000 USD) for breach of obligations in respect of children.	Processing personal data of a minor (<18) without verifiable parental consent, behavioral tracking, or targeted advertising.	Statutory 18+ Age Gate hardcoded in onboarding; refusal of minors; strict prohibition of targeted ads; zero behavioral tracking of minors.
India DPDP Act 2023 (Sec 6 & 12)	₹50 Crores (~\$6,000,000 USD) for failure to give notice/consent or failure to honor erasure.	Bundled non-consensual tracking, refusing account deletion, retaining orphaned records.	Unbundled affirmative checkboxes for Terms and Health Processing at signup; immediate complete erasure via in-app Profile and public web deletion portal.
EU & UK GDPR (Article 83(5))	€20,000,000 or 4% of total worldwide annual turnover , whichever is higher.	Processing Special Category Health Data (Art 9) without explicit consent; failure to facilitate Art 17 Right to Erasure or Art 20 Portability.	Explicit, granular Article 9 consent mechanism; automated JSON data export module; complete cloud and local storage hard-purge protocol.
California CCPA / CPRA (Cal. Civ. Code § 1798.199.90)	\$7,500 per intentional violation ; statutory civil damages for data breaches.	Selling or sharing Sensitive Personal Information (SPI) without opt-out; discrimination against consumers.	Statutory "Zero Data Sale / Zero Data Sharing" certification; limiting SPI exclusively to user-requested fitness features; non-discriminatory service tier.
US COPPA (FTC Civil Penalties)	Up to \$50,120 per violation per child.	Actual knowledge or constructive collection of child personal information (<13).	Hard 18+ adult age threshold; zero directed marketing; instant purge protocol if minor data is erroneously detected.
Google Play / Apple App Stores	Permanent developer account termination, app removal, global distribution ban.	Health Connect data passed to advertisers; undeclared sensitive permissions; missing web deletion URL.	Isolated health architecture; zero ad SDK health access; published Health Connect rationale activity; live web deletion portal at fitkobra.com.

3. DATA FIDUCIARY IDENTITY & STATUTORY OFFICER DESIGNATION

Under Section 2(i) of the DPDP Act 2023 and Article 4(7) of the GDPR, the designated legal entity determining the purpose and means of personal data processing is:

CORPORATE & DATA PROTECTION OFFICERS **Entity Name:** FitKobra AI Technologies Inc. (Operating as "FitKobra")
Designated Grievance Redressal Officer (DPDP Act Sec 8(9) & Sec 13): Grievance Officer, Privacy Operations
Data Protection Officer (DPO - GDPR Art 37): Data Protection Officer, Global Compliance

Official Statutory Contact Email: fitkobra.ai@gmail.com (Subject: "Data Protection Grievance / DSAR - Attn: Grievance Officer")

Statutory Service Level Agreements (SLAs): Formal acknowledgment within **forty-eight (48) hours**; complete investigation and binding resolution within **thirty (30) calendar days**.

Appeals Escalation Authority: Data Principals unsatisfied with internal resolution hold the statutory right to escalate directly to the **Data Protection Board of India (DPBI)** at <https://dpb.gov.in> or relevant EU Supervisory Authority.

4. EXHAUSTIVE DATA INVENTORY & LAWFUL PURPOSE MAPPING

To satisfy the statutory mandate of *Data Minimisation* (GDPR Art 5(1)(c)) and *Purpose Limitation* (DPDP Act Sec 6(1)), FitKobra categorizes all processed data into strictly defined classes. FitKobra certifies that it does NOT collect, harvest, infer, or store any data point outside this declared schedule:

DATA CATEGORY	SPECIFIC DATA POINTS	STORAGE LOCATION & PERSISTENCE	LAWFUL BASIS & EXPLICIT PURPOSE
1. Account & Identity	Email address, Full Name / Display Name, Profile Photo URL, Firebase Unique Identifier (`uid`), OAuth provider tokens.	Google Firebase Auth & Cloud Firestore users/{uid}. Encrypted at rest. Retained until account erasure.	Contractual Necessity & Authentication: Required to authenticate users, secure account boundaries, prevent account takeover, and sync cross-device fitness progression.
2. Physical & Biometrics	Date of Birth, Age, Biological Gender, Height (cm), Weight (kg), Baseline Activity Level, Primary Fitness Goal.	Cloud Firestore users/{uid} & local device cache. Retained until account erasure.	Physiological Calculation & Age Gating: Required to compute Basal Metabolic Rate (BMR) and Total Daily Energy Expenditure (TDEE), and to enforce statutory 18+ adult age requirements.
3. Cardiovascular & Vitals (Special Category)	Personal Blood Pressure logs (systolic, diastolic, mean arterial pressure), manual resting pulse cadence taps, timestamps.	Cloud Firestore users/{uid}/vitals subcollection. Fully isolatable and deletable by user.	Explicit Health Consent (GDPR Art 9 / DPDP Sec 6): Voluntary recreational athletic cardiovascular journaling. Strictly isolated from third parties, insurers, and advertising SDKs.
4. Pedometer & Motion Telemetry	Daily step counts, active minutes, estimated exercise calories, smartwatch synchronization data.	On-device Android Step Counter / Apple CoreMotion, synced to Firestore users/{uid}/dailyStats.	Activity Ring Progression: Real-time on-device physical activity tracking and milestone badges. Deduplicated using Anti-Double-Counting algorithm. Never commercialized.
5. Nutrition & Food Imagery	Meal names, portion weights, macronutrient breakdowns (protein, carbs, fat, kcal), food photo captures.	Firestore users/{uid}/meals subcollection. Photos processed ephemerally in RAM via Gemini API.	Caloric Balance Tracking: Logging nutritional intake against metabolic targets. Food photos are discarded immediately after analysis and NEVER stored permanently or used for model training.
6. Gamification &	Public Display Name, Profile	Cloud Firestore	Legitimate Interest & Consent: Optional

DATA CATEGORY	SPECIFIC DATA POINTS	STORAGE LOCATION & PERSISTENCE	LAWFUL BASIS & EXPLICIT PURPOSE
Community	Photo (Google Auth), total accumulated activity points, daily streak count.	leaderboard/{uid} collection. Visible to authenticated users.	community engagement. Sensitive health metrics, weight, and email are strictly EXCLUDED. Immediate opt-out available.

5. INDIA DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP ACT) SHIELD

FitKobra operates in strict conformance with every substantive chapter of the DPDP Act 2023. Compliance is baked into the application's software architecture as follows:

5.1 Notice and Unbundled Consent Architecture (Section 5 & Section 6)

- Unbundled Clear Notice:** In compliance with Section 5(1), before any data processing commences, FitKobra presents an itemized, unbundled notice setting out the exact personal data requested, the explicit purpose, how the Data Principal may exercise rights under Section 12, and how to lodge complaints with the Grievance Officer and Data Protection Board of India.
- Granular Affirmative Consent:** FitKobra rejects bundled pre-checked consent boxes. Registration requires independent affirmative clicks: (1) Acceptance of Terms of Service and Privacy Policy, and (2) Specific unbundled consent for collecting voluntary fitness and cardiovascular metrics.
- Unconditional Right to Withdraw Consent (Section 6(7)):** Users may withdraw consent at any time via Profile Settings. Withdrawal triggers zero penalties and immediately terminates active processing.

5.2 Absolute Minor & Child Protection Mandate (Section 9) — Zero-Tolerance Shield

STATUTORY SECTION 9 ENFORCED SAFEGUARDS Section 9 of the DPDP Act 2023 strictly prohibits processing personal data of children (<18) without verifiable parental consent, and bans behavioral tracking, profiling, or targeted advertising directed at children.

- 1. Automated 18+ Hard Gate:** During onboarding, FitKobra's date-of-birth parser calculates chronological age. If the user is under 18, account creation is blocked with a statutory alert.
- 2. Zero Targeted Ads:** FitKobra's AdMob integration passes requestNonPersonalizedAdsOnly: true for all advertising requests.
- 3. Immediate Purge Protocol:** If the Company receives notice that personal data of any minor has entered the system, all associated records across Firebase Auth, Cloud Firestore, and local caches are irreversibly purged within 24 hours.

5.3 Complete Exercise of Data Principal Rights (Sections 11, 12, 13, 14)

- Section 11 (Right to Access & Summary):** Users can generate a real-time comprehensive JSON audit report of all stored metrics via Profile → Settings → "Export My Data".
- Section 12 (Right to Correction & Erasure):** Users can edit erroneous metrics in real-time or trigger hard deletion via Profile → Settings → "Delete Account", which executes a multi-layer cascade wiping all subcollections and the primary authentication record.
- Section 13 (Right of Grievance Redressal):** Designated Grievance Officer responds to all inquiries within 48 hours and provides definitive resolution within 30 days.
- Section 14 (Right to Nominate):** Data Principals possess the statutory right to designate a legal representative or nominee to exercise privacy rights in the event of death or incapacity by filing a formal request with the Grievance Officer.

6. EUROPEAN UNION & UNITED KINGDOM GDPR COMPLIANCE SHIELD

FitKobra adheres to the highest global data privacy standards prescribed under Regulation (EU) 2016/679 and UK Data Protection Act 2018:

6.1 Special Category Health Data Explicit Consent (Article 9(2)(a))

Cardiovascular metrics (blood pressure logs and tactile pulse cadence readings) constitute Special Category Personal Data under GDPR Article 9(1). FitKobra relies strictly upon the explicit consent exception under **Article 9(2)(a)**. Users affirmatively consent before saving any vitals record, and may delete individual records or the entire vitals subcollection independently without deleting their primary athletic account.

6.2 Technical & Organizational Security Measures (TOMs - Article 32)

- **Encryption at Rest:** All Cloud Firestore documents, database partitions, and cloud backups are encrypted using Federal Information Processing Standard (FIPS) 140-2 validated AES-256 encryption.
- **Encryption in Transit:** All data transmissions between client devices and Google Cloud / Firebase servers are enforced exclusively via Transport Layer Security (TLS 1.3 / HTTPS).
- **Access Control:** Granular Cloud Firestore Security Rules enforce strict cryptographic boundary checks ensuring authenticated users can ONLY read and write documents where `request.auth.uid == userId`.

6.3 Mandatory 72-Hour Personal Data Breach Notification Protocol (Articles 33 & 34)

In the event of a confirmed personal data breach affecting users in the EU, UK, or India:

1. **Immediate Incident Containment:** Security operations isolate affected cloud endpoints within 4 hours.
2. **Statutory Authority Notification (Within 72 Hours):** Written notification detailing the nature of the breach, affected data categories, estimated number of individuals, and mitigation measures is transmitted to the competent Data Protection Authority (e.g., DPC Ireland, CNIL France, ICO UK, or DPBI India).
3. **Data Subject Direct Communication:** Where the breach poses a high risk to rights and freedoms, direct push and email notifications are dispatched immediately to all affected users with remediation guidance.

6.4 Cross-Border International Data Transfers (Chapter V & Article 46)

Personal data is processed on Google Cloud Platform enterprise infrastructure. All international transfers between India, the EU, UK, and the United States are governed by European Commission approved **Standard Contractual Clauses (SCCs)** integrated into Google Cloud's Data Processing and Security Terms, ensuring adequate protection under Schrems II guidelines.

7. UNITED STATES FEDERAL & STATE PRIVACY SHIELD (CCPA / CPRA & COPPA)

7.1 California Consumer Privacy Act (CCPA) as amended by CPRA

STATUTORY "DO NOT SELL OR SHARE" DECLARATION FitKobra hereby declares and certifies under penalty of regulatory sanctions:

1. **ZERO SALE OF PERSONAL INFORMATION:** FitKobra has NEVER sold, does NOT sell, and will NEVER sell personal information of any user to third parties, data brokers, or commercial resellers (Cal. Civ. Code § 1798.140(ad)).
2. **ZERO SHARING FOR CROSS-CONTEXT ADVERTISING:** FitKobra does NOT share personal information with third parties for cross-context behavioral advertising (Cal. Civ. Code § 1798.140(ah)).
3. **LIMITATION ON SENSITIVE PERSONAL INFORMATION (SPI):** Sensitive health and biometric metrics are processed solely to provide user-requested fitness features and are NEVER used to infer characteristics (Cal. Civ. Code § 1798.121).

4. CONSUMER STATUTORY RIGHTS: California residents hold the Right to Know, Right to Delete, Right to Correct, and Right to Non-Discrimination. Requests can be submitted via Profile or by emailing fitkobra.ai@gmail.com.

7.2 Children's Online Privacy Protection Act (COPPA)

FitKobra does not direct its service to children under thirteen (13) years of age, nor does it knowingly collect personal information from children under 13. By enforcing an automated 18+ age verification gate during account setup, FitKobra establishes complete statutory immunity under 16 C.F.R. Part 312.

8. NON-MEDICAL SAMD DISCLAIMER & ABSOLUTE LIABILITY DEFENSE

To protect FitKobra, its corporate directors, founders, and affiliates from medical malpractice claims, product liability, and FDA / CE regulatory enforcement, the following statutory disclaimers are legally binding on all users:

 **STATUTORY MEDICAL & NON-SAMD DISCLAIMER (FDA & EU MDR REGULATORY SHIELD) 1. CONSUMER WELLNESS PRODUCT ONLY:** FitKobra, its AI Coach ("Coach Maya"), meal scanning vision tools, blood pressure logger, and tactile pulse cadence rhythm checker are developed and provided STRICTLY for general recreational fitness, athletic conditioning, and personal lifestyle journaling. FitKobra is **NOT a certified medical device** and does NOT constitute Software as a Medical Device (SaMD) under US FDA regulations (21 CFR Part 860 et seq.), EU Medical Device Regulation (MDR 2017/745), Australian Therapeutic Goods Administration (TGA), or Indian Medical Devices Rules, 2017.

2. NO MEDICAL DIAGNOSIS OR CLINICAL TREATMENT: FitKobra is NOT designed, intended, cleared, or approved to screen, diagnose, treat, mitigate, or prevent any illness, disease, cardiac disorder, cardiac arrhythmia, myocardial infarction (heart attack), stroke, arterial disease, hypertension crisis, or metabolic syndrome. Nothing in the app constitutes clinical advice, nursing care, or medical diagnosis.

3. TACTILE CADENCE PULSE STANDARD: Pulse rhythm checks are derived exclusively from manual user touch taps synchronized with physical pulse palpation (radial or carotid artery) following American Heart Association (AHA) athletic guidelines. FitKobra does NOT utilize optical camera sensors, infrared photoplethysmography (PPG), or LED flash illumination for pulse detection.

4. MANDATORY EMERGENCY MEDICAL PROTOCOL: If you experience severe chest pain, pressure radiating to the jaw, neck, back, or arm, sudden shortness of breath, unexplained fainting, lightheadedness, or acute hypertensive readings (>180 systolic or >120 diastolic mmHg), **IMMEDIATELY CALL LOCAL EMERGENCY MEDICAL SERVICES (911 in the USA/Canada, 112 in the European Union and India, 000 in Australia, 999 in the United Kingdom)**. Never delay or disregard emergency clinical intervention based on metrics within FitKobra.

5. COMPLETE ASSUMPTION OF PHYSICAL RISK & INDEMNIFICATION: Physical exercise and athletic training involve inherent risks of cardiovascular strain, muscle tearing, skeletal injury, and unforeseen physical complications. You voluntarily assume all risks associated with your workouts. To the fullest extent permitted by law, you agree to release, waive, defend, and hold harmless FitKobra AI Technologies Inc., its directors, employees, and software architects from any liability, injury, illness, death, or damage arising directly or indirectly from use of the application.

9. GOOGLE PLAY & APPLE APP STORE PLATFORM POLICY HARMONIZATION

9.1 Google Play Health Connect Policy Compliance

- **Strict Purpose Limitation:** Permissions for `android.permission.health.READ_STEPS` and `android.permission.health.READ_TOTAL_CALORIES_BURNED` are requested solely to populate real-time

activity rings and calculate daily caloric burn.

- **Zero Advertising Use:** FitKobra guarantees that data obtained through Health Connect is NEVER sold, transferred to data brokers, or utilized for advertising or marketing purposes.
- **Health Connect Permission Usage Rationale:** Build 249+ declares the required `ViewPermissionUsageActivity` alias in `AndroidManifest.xml`, routing users directly to the in-app Privacy Policy.

9.2 Google Play Account Deletion Policy Compliance (Dual-Portal Guarantee)

Google Play requires apps enabling account creation to provide both an in-app deletion path and a public web deletion URL:

- **In-App Deletion Path:** Profile → Settings → "Delete Account & Data" triggers an immediate permanent wipe of Firestore documents, subcollections (meals, vitals, dailyStats, workouts, goals), leaderboard entries, and Firebase Auth credentials.
- **Public Web Deletion Portal:** Available at <https://www.fitkobra.com/#data-deletion> and within <https://www.fitkobra.com/privacy.html>, enabling users to submit account deletion requests without having the app installed. Requests are verified and completed within 48 to 72 hours.

9.3 Google AdMob Policy & Non-Personalized Ads Shield

- **Non-Personalized Configuration:** All ad requests initialize with `requestNonPersonalizedAdsOnly: true`, insulating the app from profiling liabilities.
- **App-Ads.txt Authentication:** Verified developer ownership via `fitkobra.com/app-ads.txt` containing Google AdMob publisher ID `pub-9025413323620577`.
- **Complete Health-to-Ad Isolation:** No health, vitals, pedometer, or nutrition records are accessible to or shared with the AdMob SDK.

10. CODEBASE AUDIT FINDINGS & IMMEDIATE STATUTORY REMEDIATIONS

An exhaustive compliance audit of the FitKobra codebase (FitKobra Core Mobile Application, Android Manifest, and Web Portal) identified four (4) critical areas requiring immediate remediation to eliminate Google Play hold risks and statutory privacy liabilities:

AUDIT FINDING & FILE LOCATION	COMPLIANCE RISK & STATUTORY EXPOSURE	REQUIRED REMEDIATION ACTION	REMEDIAL STATUS
Finding 1: Unused Restricted Permissions android/app/src/main/AndroidManifest.xml Lines 11 & 17: android.permission.BODY_SENSORS android.permission.SYSTEM_ALERT_WINDOW	High Google Play Store Rejection Risk: BODY_SENSORS is a restricted health permission requiring video proof of hardware sensor usage. Since FitKobra uses manual tap cadence, requesting it triggers automated policy rejections. SYSTEM_ALERT_WINDOW ("Draw over other apps") is restricted and disallowed in	IMMEDIATE ACTION: Remove both BODY_SENSORS and SYSTEM_ALERT_WINDOW from android/app/src/main/AndroidManifest.xml. Maintain only ACTIVITY_RECOGNITION (used for pedometer) and Health Connect step permissions.	ACTION REQUIRED

AUDIT FINDING & FILE LOCATION	COMPLIANCE RISK & STATUTORY EXPOSURE	REQUIRED REMEDIATION ACTION	REMEDIAL STATUS
	release builds.		
	DPDP Sec 12 / GDPR Art 17		
	Violation:		
	While		
Finding 2: Incomplete Deletion in EditProfileModal	app/(tabs)/profile.tsx	IMMEDIATE ACTION: Update	
components/EditProfileModal.tsx	calls deleteUserData(uid)	handleDeleteAccount in	
Line 86	and	components/EditProfileModal.	
	resetLocalSessionData(u	tsx to invoke	ACTION
	id) before	resetLocalSessionData(uid)	REQU
	deleteAccount(),	and deleteUserData(uid) prior to	
	EditProfileModal.tsx	Auth deletion, mirroring the robust	
	only calls deleteAccount().	logic in profile.tsx.	
	This leaves orphaned Firestore		
	documents in breach of Right		
	to Erasure mandates.		
	Regulatory & Store Review		
	Conflict:		
	The website modals still		
Finding 3: Disparity in Website Legal Modals	referenced legacy "Optical	IMMEDIATE ACTION: Update	
fitkobra_website/src/components/Privacy	Camera PPG Pulse Check	PrivacyPolicyModal.jsx and	
PolicyModal.jsx &	using LED Flash", whereas the	TermsOfServiceModal.jsx to	ACTION
TermsOfServiceModal.jsx	app and	match public/privacy.html,	REQU
	public/privacy.html	confirming pulse measurement is	
	explicitly specify manual tactile	manual tactile tap cadence with zero	
	tap cadence. Conflicting	camera/flash usage.	
	disclosures trigger SaMD		
	medical scrutiny during store		
	reviews.		
	Bot & Abuse Prevention:		
Finding 4: Web Deletion Portal Firestore Protection	Public deletion form pushes to	RECOMMENDED ACTION: Ensure	
fitkobra_website/src/components/DataDel	deletion_requests	Firestore rules enforce	
etionModal.jsx	collection. Without strict rate	request.resource.data.keys()	PROTE
	limiting or schema validation	.hasAll(['email', 'status',	
	rules in Firestore security	'requestedAt']) and string length	
	rules, malicious actors could	limits on deletion_requests.	
	spam invalid emails.		

11. STATUTORY EXECUTION & CORPORATE CERTIFICATION

FitKobra AI Technologies Inc. certifies that this document represents the comprehensive, accurate, and operative legal framework governing all production software builds, data pipelines, and third-party integrations. Any modification to data storage, third-party sub-processors, or biometric processing must be reflected in an updated revision of this charter and

published across both in-app legal endpoints and the live domain at <https://www.fitkobra.com>.

Executed		and		Certified		by:
FitKobra	Compliance		&	Data	Protection	Directorate
FitKobra		AI		Technologies		Inc.
Official	Record	Date:		September	23,	2026
Governing Registry: fitkobra.ai@gmail.com https://www.fitkobra.com/privacy						