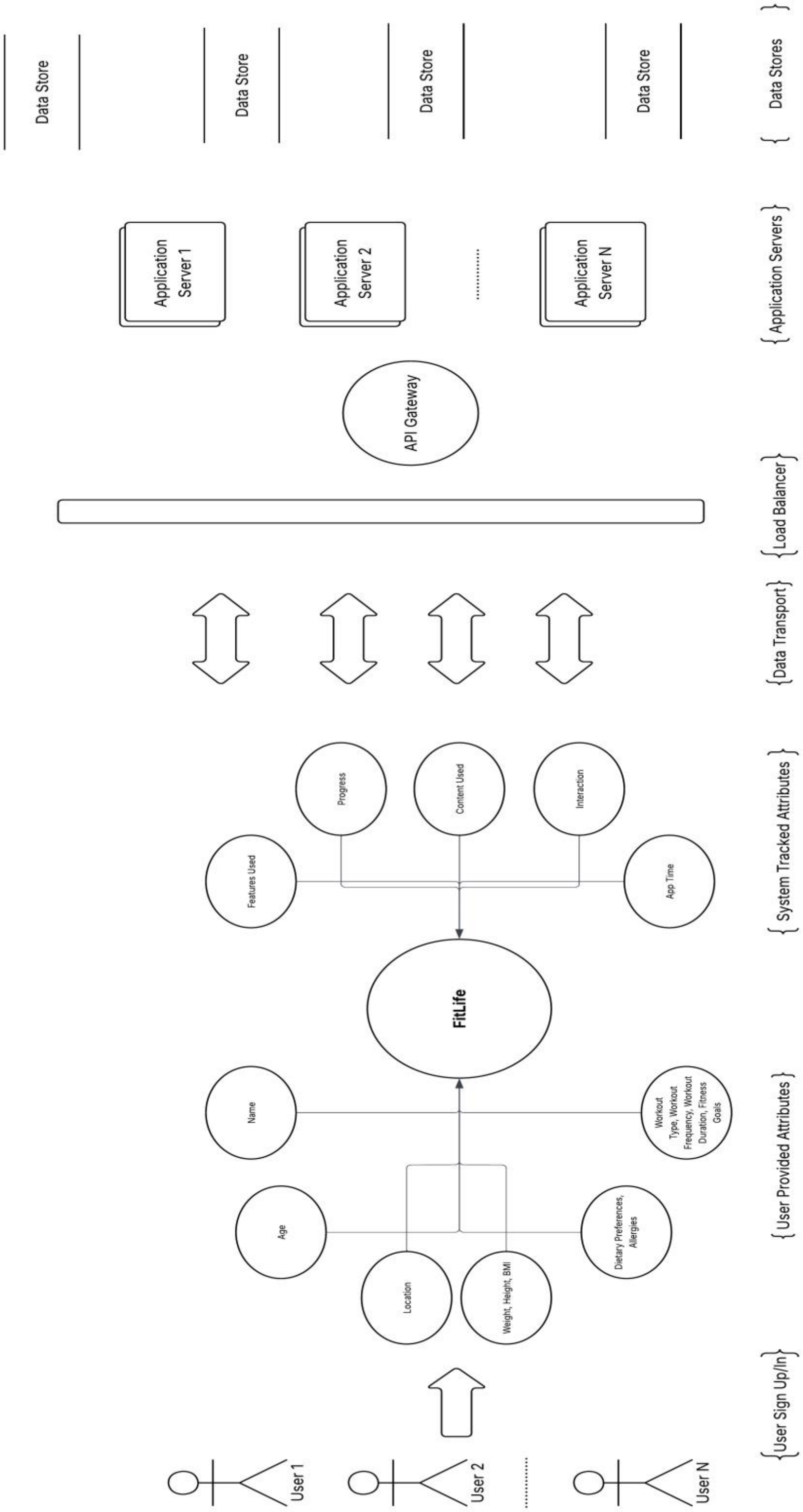
FitLife - Personalized nutritionist

FitLife collects user data, including health statistics, dietary habits, and workout routines, to provide personalized fitness and nutrition plans. It also offers community features, allowing users to connect with each other, share their progress, and even engage in friendly competition.

Section 1: Dataset

Column Name	Description	Data Type	identifier
Name	User’s Full Name	String	**Direct Identifier**
Age	User’s Age in years	Number	**Indirect Identifier**
Location	User’s City and Country of Residence	String	**Indirect Identifier**
Gender	User’s Gender	Enumeration	**Indirect Identifier**
Weight	User’s Body weight in Kilograms	Number	**Indirect Identifier**
Height	User’s Height in centimeters	Number	**Indirect Identifier**
BMI	User’s Body Mass Index	Number	**Indirect Identifier**
Dietary Preference	User’s Dietary Preference	String	**Indirect Identifier**
Allergies	User’s Food Allergies	String	**Indirect Identifier**
Workout Frequency	Number of Workout Sessions of the User in a Week	Number	**Indirect Identifier**
Workout Type	Preffered Workout Type of the User	String	**Indirect Identifier**
Workout Duration	Average Workout Duration of each Session in minutes	Number	**Indirect Identifier**
Fitness Goals	Fitness objective of the User	Enumeration	**Indirect Identifier**
Progress	System tracked Fitness Progress of the User	Enumeration	**Indirect Identifier**
Features Used	App functionalities used by the User	Enumeration	**Indirect Identifier**
App Time	Average time spend on the Application in minutes	Number	**Indirect Identifier**
Interaction	Form of User Interaction on the Application	Enumeration	**Indirect Identifier**
Content Preference	Content Preffered by the User on the Application	Enumeration	**Indirect Identifier**

Section 2: System Reference Diagram (link)



Section 3: LINDDUN Threat Categories

1. **LINKABILITY**
    a. **Hotspot - Data collection for account registration**
        i. **Threat -** Same user data (Name, Age, Location) can be linked across entries related through friendship(connection) link.
    b. **Hotspot - Data Storage (Data Stores)**
        i. **Threat -** Repeated workout or usage of app can link the user's activity over the time.
2. **IDENTIFIABILITY**
    a. **Hotspot - Data Collection for account registration**
        i. **Threat -** Using real names and detailed location makes user easily identifiable.
    b. **Hotspot - Data Storage (Data Stores)**
        i. **Threat -** Combination of data points (Height, Weight, Location could be used to identify a user, if the data is leaked).
        ii. **Threat -** Misuse of Dangerous Data (Dietary Preferences) can be used to target a user.
3. **NON-REPUDIATION**
    a. **Hotspot - Application Servers**
        i. **Threat -** All activities are recorded by the user (Workout Duration, Workout Type, Workout Frequency).
4. **DETECTABILITY**
    a. **Hotspot - Data Transmission (Application -> Servers)**
        i. **Threat -** Man in the Middle attack, can possibly know when the user is online and working out.
    b. **Hotspot - Data Transmission (Servers -> Application)**
        i. **Threat -** Notifications can reveal sensitive details about the user.
5. **UNAWARENESS**
    a. **Hotspot - Continuous Sync**
        i. **Threat -** User's don't know that their fitness data keeps syncing automatically.
    b. **Hotspot - Usage Tracking**
        i. **Threat -** User might not be aware that the app tracks what features or other things they interact with.
6. **NON-COMPLIANCE**
    a. **Hotspot - Data Storage (Data Stores)**
        i. **Threat -** Old user's data might not be deleted on time.
        ii. **Threat -** Linking one user's data with other user's data without clearly asking for consent from the users.
    b. **Hotspot - Data Collection**
        i. **Threat -** User's might not clearly agree before sharing their health data.

7. DISCLOURSE OF INFORMATION

a. Hotspot - Data Storage (Data Stores)

i. **Threat -** Poor access control can lead to exposure of other users’ personal health data.

Section 4: ARX Certificate - (ATTACHED CERTIFICATE FILE)

Section 5: Explanation of ARX Configuration Decisions

Input Specifications

The dataset includes **500 individual records** with **18 attributes** covering identification, demographic, and health or fitness information.

Classification	Attributes	Rationale
Identifying	Name	Directly identifies individuals. This attribute is removed from the anonymized dataset to prevent instant identification.
Quasi-Identifying	Age, Location, Gender	These demographic details can indirectly reveal identities when linked with external sources such as public records or social media.
Sensitive	Weight, Height, BMI, Workout Frequency, Workout Type, Workout Duration, Content Preference, Interaction, Allergies	These attributes reflect health status, fitness behavior, and medical conditions.
Insensitive	Progress, Fitness Goals, Features Used, Dietary Preference, App Time(minutes)	These are general usage and preference data points. They pose minimal privacy risk and help maintain the analytical utility of the dataset.

Privacy Models Applied:

1. k-Anonymity (k=10)

Each combination of quasi-identifiers (Age, Location, Gender) appears in at least **10 records**.This ensures that no individual can be uniquely identified based on demographic combinations alone.

2. ℓ-Diversity Models (for variety protection)

Ensures variety of values within groups, preventing homogeneity attacks where all members share similar behaviors/conditions

Attribute	ℓ Value	Justification
Workout Duration	10	High diversity required due to its strong behavioral uniqueness. Prevents homogeneity attacks.
Content Preference	3	Guarantees that all three preference categories are represented in each group.
Workout Type, Interaction, Allergies	3	Provides standard diversity for categorical sensitive attributes.

3. t-Closeness Models (for distribution protection)

Prevents attackers from inferring sensitive information by ensuring that attribute distributions within each group are similar to the overall dataset.

Attribute	t Value	Justification
Weight	0.3	Strong protection for stigmatized or sensitive health metrics. Prevents skewed clusters.
BMI, Height, Workout Duration	0.4	Moderate protection for correlated attributes to balance privacy with data usability.

Output Properties

- **Data Preservation:** 500 records retained (100%)
- **Attributes maintained:** All 18 columns kept after anonymization

Applied Transformations:

- **Quasi-identifiers:** (Age, Location, Gender) were generalized to their maximum levels.
- **Sensitive attributes:** retained their original values but were protected by the chosen privacy models.

Privacy Guarantees:

- **k-anonymity (k=10):** Each record is indistinguishable from at least 9 others.
- **ℓ-diversity:** All equivalence classes meet the required diversity levels for sensitive attributes.
- **t-closeness:** Attribute distributions remain within the defined similarity thresholds.
- **Re-identification risk:** Below 10% across all modeled attack scenarios.

Model Performance

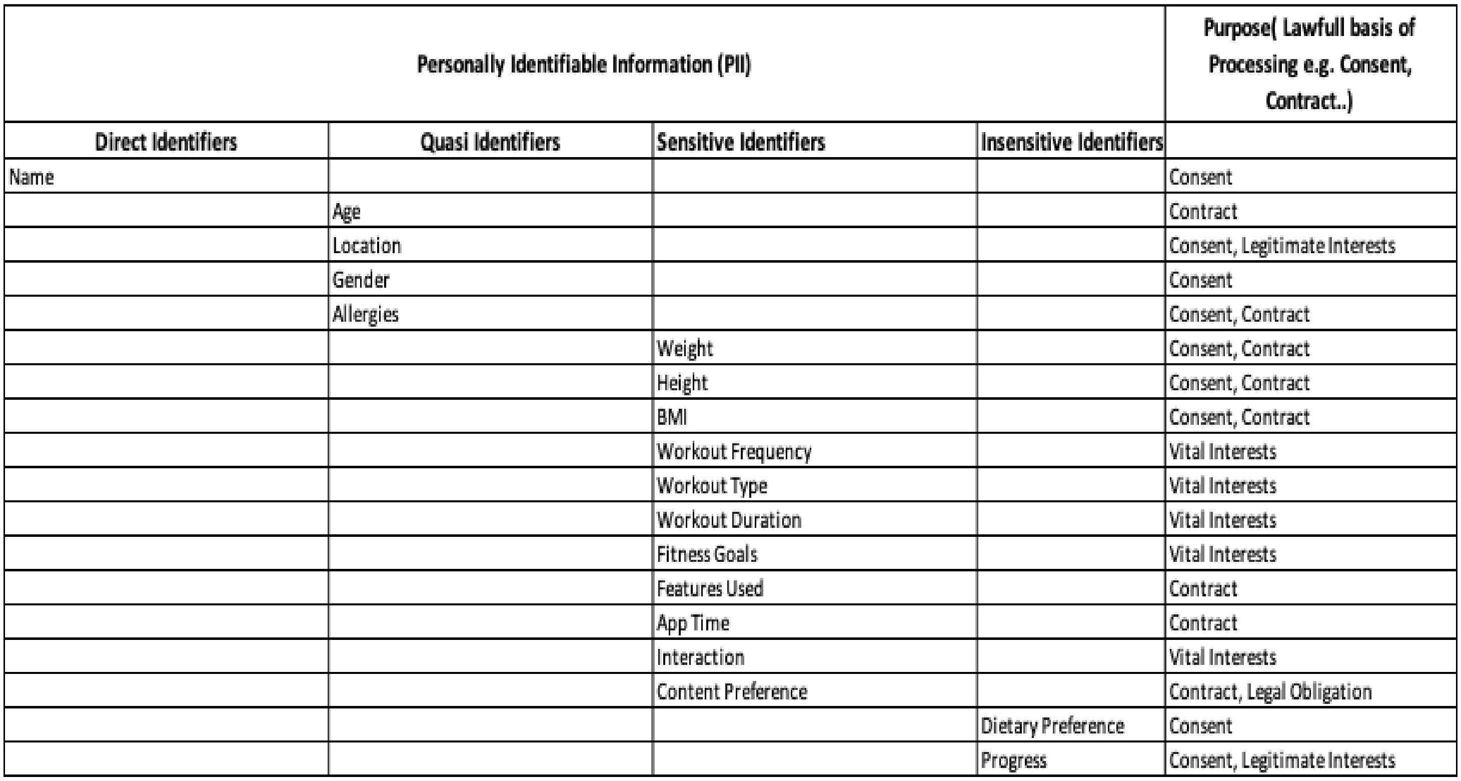
- **Transformations Evaluated:** 938 possible combinations explored
- **Final Solution:** Achieved optimal balance between privacy and data utility (Anonymity = Yes)
- **Information Loss:** Normalized score of 1.0, considered acceptable given the high privacy protection levels.

Section 6: Solutions for the Threats outlined in Section 3

- **Hotspot - Data collection for account registration**
    - **Threat -** Same user data (Name, Age, Location) can be linked across entries related through friendship(connection) link.
        - **Solution -** We will be using the separation of responsibility technique while handling data regarding the User Profile (Name, Age and Location) so that a single service will have access over this data and to create friendship (connections) this would be responsible by another service. Single Service – Single Responsibility – Single Database Access
- **Hotspot - Data Storage (Data Stores)**
    - **Threat -** Repeated workout or usage of app can link the user's activity over the time.
        - **Solution –** This data will be stored encrypted in our database with minimum data retention policies (auto deletion of old processed data).
- **Hotspot - Data Collection for account registration**
    - **Threat -** Using real names and detailed location makes user easily identifiable.
        - **Solution -** Generalize location (as we are already doing in the provided dataset).
- **Hotspot - Data Storage (Data Stores)**
    - **Threat -** Combination of data points (Height, Weight, Location could be used to identify a user, if the data is leaked).
        - **Solution -** As pointed out above in the User Profile data, we will be storing this data separately than the User Profile data with different access controls
    - **Threat -** Misuse of Dangerous Data (Dietary Preferences) can be used to target a user.
        - **Solution -** This data will have a limited use, state the only use to the User to create a Metric for Fitness Goal
- **Hotspot - Application Servers**
    - **Threat -** All activities are recorded by the user (Workout Duration, Workout Type, Workout Frequency).
        - **Solution -** Apply Data Minimization, log the most necessary events only. Before Publishing them for analysis Anonymize them
- **Hotspot - Data Transmission (Application -> Servers)**
    - **Threat -** Man in the Middle attack, can possibly know when the user is online and working out.
        - **Solution -** Implement TLS for all data transmission between the Application and the Servers, also use Certificate Pinning in Mobile Application to verify the authenticity of the Servers
- **Hotspot - Data Transmission (Servers -> Application)**
    - **Threat -** Notifications can reveal sensitive details about the user.
        - **Solution -** Use Asymmetric encryption to deliver notification payload to the Application

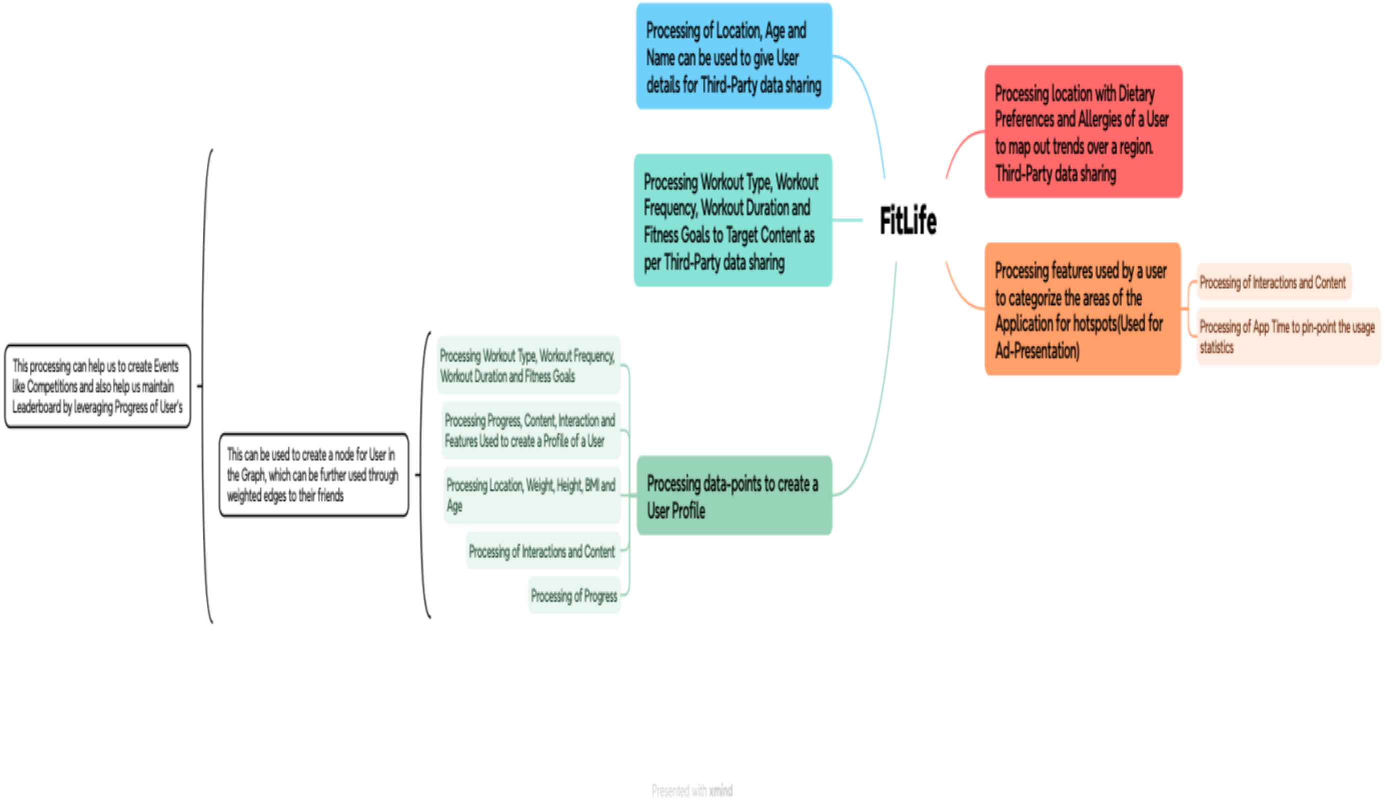
- **Hotspot - Continuous Sync**
    - **Threat -** User's don't know that their fitness data keeps syncing automatically.
        - **Solution -** Display Clear Sync Jobs Status on the Application Homepage
- **Hotspot - Usage Tracking**
    - **Threat -** User might not be aware that the app tracks what features or other things they interact with.
        - **Solution -** Keep Tracking off by default. Give User control to the minute Tracking settings.
- **Hotspot - Data Storage (Data Stores)**
    - **Threat -** Old user's data might not be deleted on time.
        - **Solution -** Create an independent Service whose sole purpose is to implement automated data cleanup jobs.
    - **Threat -** Linking one user's data with other user's data without clearly asking for consent from the users.
        - **Solution -** Clearly state this in the Privacy Policy and before any processing on this data (like processing on health data below) sent a notification through different channels to the User indicating about it. The User should also have the say to always stop the processing and storage.
- **Hotspot - Data Collection**
    - **Threat -** User's might not clearly agree before sharing their health data.
        - **Solution -** Clearly state this in the Privacy Policy and before any processing on this data sent a notification through different channels to the User indicating about it.
- **Hotspot - Data Storage (Data Stores)**
    - **Threat -** Poor access control can lead to exposure of other users' personal health data.
        - **Solution -** Use Role Based Access Control and give the least required access. Also apply encryption at rest (for storing information in the Data-Store)

Section 7.1: Spread Sheet of Data Inventory



Personally Identifiable Information (PII)				Purpose(Lawfull basis of Processing e.g. Consent, Contract..)
Direct Identifiers	Quasi Identifiers	Sensitive Identifiers	Insensitive Identifiers	
Name				Consent
	Age			Contract
	Location			Consent, Legitimate Interests
	Gender			Consent
	Allergies			Consent, Contract
		Weight		Consent, Contract
		Height		Consent, Contract
		BMI		Consent, Contract
		Workout Frequency		Vital Interests
		Workout Type		Vital Interests
		Workout Duration		Vital Interests
		Fitness Goals		Vital Interests
		Features Used		Contract
		App Time		Contract
		Interaction		Vital Interests
		Content Preference		Contract, Legal Obligation
			Dietary Preference	Consent
			Progress	Consent, Legitimate Interests

Section 7.2: Data Processing Register (**Added in the Excel Sheet)**



FitLife

Processing of Location, Age and Name can be used to give User details for Third-Party data sharing

Processing Workout Type, Workout Frequency, Workout Duration and Fitness Goals to Target Content as per Third-Party data sharing

Processing data-points to create a User Profile

Processing Workout Type, Workout Frequency, Workout Duration and Fitness Goals

Processing Progress, Content, Interaction and Features Used to create a Profile of a User

Processing Location, Weight, Height, BMI and Age

Processing of Interactions and Content

Processing of Progress

This can be used to create a node for User in the Graph, which can be further used through weighted edges to their friends

This processing can help us to create Events like Competitions and also help us maintain Leaderboard by leveraging Progress of User's

Processing location with Dietary Preferences and Allergies of a User to map out trends over a region. Third-Party data sharing

Processing features used by a user to categorize the areas of the Application for hotspots(Used for Ad-Presentation)

Processing of Interactions and Content

Processing of App Time to pin-point the usage statistics

Picture 1: Screenshot from X-Mind Application(used for Brainstorming Ideas)

Section 7.3: Privacy Policy and Terms Of Use (Inspired from Strava)

Privacy Policy

Information FitLife Collects

FitLife collects information about you, including information that directly or indirectly identifies you, if you or other FitLife users choose to share it with FitLife. The sources from which we collect this personal information fall into four categories: Identifying Information, Quasi-Identifying Information, Sensitive Information and In-Sensitive Information. These informations are mostly provided to us by you or we collected it automatically when you agreed on sharing them with us. We also collect information about you from other sources. For example, based on how you interact with FitLife and the Features , we may collect information about how you use the Features. In addition, you may choose to share information about yourself, your friends and your activities with FitLife.

Account, Profile and User Activity

We collect account information such as your name, age, gender, weight, allergies, height and fitness goals that helps secure and provide you with access to our Features and Services.

Profile, activity and use information is collected about you when you engage in activities such as Workouts, Interaction with Posts, Join a Competition, View other's Posts/Content or otherwise use the Features of FitLife

Location and Workout Information

We collect and process location and workout information when you sign up for and use the Service. We do not trak your device location while you are not using the FitLife Application. In order for most of our core features(e.g., Workout Frequency tracking, Workout type tracking, Workout Duration tracking, segmnent leaderboards) to function, you must grant us permissions in your device's privacy controls to track your device location while you use the Services

If you would like to stop the device location tracking, you may do so at any time by adjusting your device settings.

Terms Of Use

These Terms of Use govern your access to and use of the FitLife platform, including the related mobile applications, products, websites, technology, software and services.

Agreement

These Terms are a binding agreement (contract) between you and FitLife. You indicate your acceptance of these Terms by accessing, using, or signing up for any Services(e.g., Competitions and other Features in the Application). If you do not agree to these Terms, do not access, use, or sign up for any Services.

NOTICE REGARDING DISPUTE RESOLUTION: THESE TERMS CONTAIN PROVISIONS THAT GOVERN HOW DISPUTES BETWEEN YOU AND FITLIFE ARE RESOLVED, INCLUDING AN AGREEMENT TO ARBITRATE, WHICH WILL-UNLESS YOU RESIDE IN THE EU OR JURIDICTIONS WHERE PROBHITED-WITH LIMITED EXCEPTION, REQUIRE YOU TO SUBMIT CLAIMS YOU HAVE AGAINST US TO BINDING AND FINAL ARBITRATION AND LIMIT YOU TO CLAIMS AGAINST FITLIFE ON AN INDIVIDUAL BASIS, UNLESS YOU OPT-OUT IN ACCORDANCE WITH THE INSTRUCTIONS BELOW.

Account

The Application of FitLife and it's Services are only intended for persons who are atleast 13 years old, or such higher age as may be required in your jurisdiction. If you are under the legal age to form alegally binding contract inyour jurisdiction, you may use the Services and the application only with the permission of your parent or legal guardian. If you area parent or a legal guardian of a FitLife user under the legal age to form abinding contract in your jurisdiction, you agree to befully responsible for the acts or omissions of such user, including any breach of these Terms.

Security

You are fully responsible for maintaing the confidentiality of your account credentials and preventing unauthorized acces to your account. You accept full responsibilty for all activites that occur under your account or from your devices.

You agree to notify FitLife immediately of any unauthorized access of your account or password, or any other breach of security. Unauthorized access to your account could expose your User Data and any other information of content you provide to FitLife to unwanted or unintended third parties.

Section 7.4: Guideline for Obtaining and Maintaining Consent

In order to adhere to Data Privacy by Design principles, FitLife considers consent as an ongoing user-controlled process instead of a one-time event. Consent is always obtained without ambiguity through clear, specific and granularity- based prompts that inform the user in advance why every category of data is being collected and how that data is going to be used. The user will be notified of any new processing activity before that activity begins, and consent can be withdrawn any time without losing access to core features. FitLife preserves an auditable consent log, regularly revalidates permissions for sensitive data, and offers simple in-app settings to review and manage tracking, data share, and personalization options. This approach allows for transparency, user control and on-going accountability throughout the entire data lifecycle.