A **smartphone application** that obtains a **clear affirmative act** to use **precise geolocation data** typically follows industry best practices to ensure **explicit user consent**. Below is an example of how a well-designed app handles this process:

Example: SecureMaps – A Location-Based Navigation App

Step 1: Pre-Permission Context (User Awareness)

Before requesting access, the app explains **why location data is needed**.

Example Popup Before Permission Request:

"SecureMaps needs access to your precise location to provide real-time navigation and location-based alerts. You can manage your preferences in settings anytime."

User Action: "Continue" (to proceed to actual permission request).

Step 2: Explicit Permission Request (OS-Level Prompt)

After providing context, the app triggers the **official OS permission prompt** for precise location access.

iOS Example Prompt:

"Allow SecureMaps to use your location?"

- **"Allow While Using App"**
- **"Allow Once"**
- **"Don't Allow"**

Android Example Prompt:

"Allow SecureMaps to access this device's location?"

- **"While Using the App"**
- **"Only This Time"**
- **"Deny"**

User Action: *Must select a positive option to proceed.*

Step 3: Additional Consent for Background Location (If Needed)

If the app requires **background location tracking**, it **must obtain separate explicit consent**.

Example Prompt:

"SecureMaps needs access to your location even when the app is closed to provide turn-by-turn directions and nearby alerts."

- **"Allow Always"**
- **"Only While Using the App"**
- **"Don't Allow"**

User Action: *Must opt-in separately for continuous tracking.*

Step 4: Clear Opt-Out & Data Control

The app includes **easy-to-access settings** for users to revoke or modify location access.

Example Path: Settings > Privacy > Location Access > Manage Permissions

User Control: Users can disable **precise location** or revoke permissions at any time.

Why This Meets Legal & Ethical Standards

Explicit user consent via an **affirmative act** (*tapping "Allow" or equivalent*).

Clear purpose explanation before requesting access.

Separate consent for background tracking (if applicable).

Easy opt-out with control over settings.

This approach **complies with GDPR, CCPA, and Apple/Google privacy policies** by ensuring **users actively approve** location tracking with a **clear affirmative action**.