# Protecting the User's Privacy

Secure personal data, and respect user preferences for how data is used.

## Overview

Designing for user privacy is important. Most Apple devices contain personal data that the user doesn't want to expose to apps or to external entities. If your app accesses or uses data inappropriately, the user might stop using your app and even delete it from their device.

Access user or device data only with the user's informed consent obtained in accordance with applicable law. In addition, take appropriate steps to protect user and device data, and be transparent about how you use it.

## Review Guidelines from Government and Industry Sources

Consult these documents:

- Mobile Privacy Disclosures: Building Trust Through Transparency. The Federal Trade Commission's report on mobile privacy.
- Opinion 02/2013 on Apps on Smart Devices. The EU Data Protection Commissioners' opinion on data protection for mobile apps.
- Privacy on the Go: Recommendations for the Mobile Ecosystem. The California State Attorney General's recommendations for mobile privacy.
- Smartphone Privacy Initiative (2012) in English or Japanese and Smartphone Privacy Initiative II (2013) in English or Japanese. The Japanese Ministry of Internal Affairs and Communications' Smartphone Privacy Initiatives.

## Request Access Only When Your App Needs the Data

Request access to sensitive user or device data—like location, contacts, and photos—at the time your app needs the data. Supply a purpose string (sometimes called a usage description string) in your app's `Information Property List` that the system can present to a user explaining why your app needs access. Provide reasonable fallback behavior in situations where the user doesn't grant access to the requested data. For more details, see Requesting access to protected resources.

## Be Transparent About How Data Will Be Used

For example, when you submit your app to the App Store, specify a URL for your privacy policy or statement as part of your App Store Connect metadata. You can also summarize that policy or statement in your app description.

## Give the User Control Over Data and Protect Data You Collect

Respect the user's preferences, and take reasonable steps to protect the data that you collect in your apps:

- Provide settings that allow the user to disable access to sensitive information. The operating system does this automatically for protected system resources—like location, contacts, and health data—through the Privacy menu of the Settings app. Extend this behavior to any data you cache from these sources or collect directly. For example, if your users build a social media profile containing personal information, offer them a way to delete the data (including any server copies you have).
- When storing files in iOS, use the strongest data protection level that works for your app, as described in Encrypting Your App's Files. Use App Transport Security when sending user or device data over the network, as described in NSAppTransportSecurity.
- If your app uses the `ASIdentifierManager` class, respect the value of its `isAdvertisingTrackingEnabled` property. If the user sets that property to false, then use the `ASIdentifierManager` class only for limited advertising purposes, like frequency capping, attribution, conversion events, estimating the number of unique users, advertising fraud detection, and debugging. See the AdSupport framework for additional information.
- If you must identify users persistently, use the `identifierForVendor` property of the `UIDevice` class or the `advertisingIdentifier` property of the `ASIdentifierManager` class.

## Use the Minimum Amount of Data Required

Request and use the minimum amount of user or device data needed to accomplish a given task. Don't seek access to or collect data for unnecessary or non-obvious reasons, or because you think it might be useful later.

If your app supports audio input, configure your audio session for recording only at the point where you actually plan to begin recording. Don't configure your audio session for recording at launch time if you don't plan to record right away. The system alerts users when apps configure their audio session for recording and gives the user the option to disable recording for your app.

# Topics

## Supporting Privacy

- Requesting access to protected resources

  Provide a purpose string that explains to a person why you need access to protected resources on their device.

- Encrypting Your App's Files

  Protect the user's data in iOS by encrypting it on disk.

# See Also

## Essentials

- Adopting Liquid Glass

  Find out how to bring the new material to your app.

- UIKit updates

  Learn about important changes to UIKit.

- About App Development with UIKit

  Learn about the basic support that UIKit and Xcode provide for your iOS and tvOS apps.