# User Data

You must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing the access, collection, use, handling, and sharing of user data from your app, and limiting the use of the data to the policy compliant purposes disclosed. Please be aware that any handling of personal and sensitive user data is also subject to additional requirements in the "Personal and Sensitive User Data" section below. In addition to this and the other Play developer program policies, you must at all times comply with privacy and data protection laws applicable in the jurisdictions in which you offer your products or services. For example, if you offer your services to users in the European Union, note that the French Data Protection Authority (CNIL) adopted guidance on best practices for protection of personal data within the mobile environment that may be helpful for you to refer to.

If you include third party code (for example, an SDK) in your app, you must ensure that the third party code used in your app, and that third party's practices with respect to user data from your app, are compliant with Google Play Developer Program policies, which include use and disclosure requirements. For example, you must ensure that your SDK providers do not sell personal and sensitive user data from your app. This requirement applies regardless of whether user data is transferred after being sent to a server, or by embedding third-party code in your app.

COLLAPSE ALL EXPAND ALL

### Personal and Sensitive User Data

Personal and sensitive user data includes, but isn't limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts, device location, SMS and call-related data, health data, Health Connect data, inventory of other apps on the device, microphone, camera, and other sensitive device or usage data. If your app handles personal and sensitive user data, then you must:

- Limit the access, collection, use and sharing of personal and sensitive user data acquired through the app to app and service functionality and policy-conforming purposes reasonably expected by the user:
  - Apps that extend usage of personal and sensitive user data for serving advertising must comply with Google Play's Ads policy.
- You may also transfer data as necessary to service providers or for legal reasons such as to comply with a valid governmental request, applicable law, or as part of a merger or acquisition with legally adequate notice to users.
- Handle all personal and sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).
- Use a runtime permissions request whenever available, prior to accessing data gated by Android permissions .
- Not sell personal and sensitive user data.
  - "Sale" means the exchange or transfer of personal and sensitive user data to a third party for monetary consideration.
    - User-initiated transfer of personal and sensitive user data (for example, when the user is using a feature of the app to transfer a file to a third party, or when the user chooses to use a dedicated purpose research study app), is not regarded as sale.

### Prominent Disclosure & Consent Requirement

In cases where your app's access, collection, use, or sharing of personal and sensitive user data may not be within the reasonable expectation of the user of the product or feature in question (for example, if data collection occurs in the background when the user is not engaging with your app), you must meet the following requirements:

**Prominent disclosure: You must provide an in-app disclosure of your data access, collection, use, and sharing. The in-app disclosure:**

- Must be within the app itself, not only in the app description or on a website;
- Must be displayed in the normal usage of the app and not require the user to navigate into a menu or settings;
- Must describe the data being accessed or collected;
- Must explain how the data will be used and/or shared;

- Cannot only be placed in a privacy policy or terms of service; and
- Cannot be included with other disclosures unrelated to personal and sensitive user data collection.

**Consent and runtime permissions: Requests for in-app user consent and runtime permission requests must be immediately preceded by an in-app disclosure that meets the requirement of this policy. The app's request for consent:**

- Must present the consent dialog clearly and unambiguously;
- Must require affirmative user action (for example, tap to accept, tick a check-box);
- Must not interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent;
- Must not use auto-dismissing or expiring messages as a means of obtaining user consent; and
- Must be granted by the user before your app can begin to collect or access the personal and sensitive user data.

Apps that rely on other legal bases to process personal and sensitive user data without consent, such as a legitimate interest under the EU GDPR, must comply with all applicable legal requirements and provide appropriate disclosures to the users, including in-app disclosures as required under this policy.

To meet policy requirements, it's recommended that you reference the following example format for Prominent Disclosure when it's required:

- "[This app] collects/transmits/syncs/stores [type of data] to enable ["feature"], [in what scenario]."
- *Example: "Fitness Funds collects location data to enable fitness tracking even when the app is closed or not in use and is also used to support advertising."*
- *Example: "Call buddy collects read and write call log data to enable contact organization even when the app is not in use."*

If your app integrates third party code (for example, an SDK) that is designed to collect personal and sensitive user data by default, you must, within 2 weeks of receipt of a request from Google Play (or, if Google Play's request provides for a longer time period, within that time period), provide sufficient evidence demonstrating that your app meets the Prominent Disclosure and Consent requirements of this policy, including with regard to the data access, collection, use, or sharing via the third party code.

Examples of common violations

### Restrictions for Personal and Sensitive Data Access

In addition to the requirements above, the table below describes requirements for specific activities.

| Activity | Requirement |
|---|---|
| Your app handles financial or payment information or government identification numbers | Your app must never publicly disclose any personal and sensitive user data related to financial or payment activities or any government identification numbers. |
| Your app handles non-public phonebook or contact information | We don't allow unauthorized publishing or disclosure of people's non-public contacts. |
| Your app contains anti-virus or security functionality, such as anti-virus, anti-malware, or security-related features | Your app must post a privacy policy that, together with any in-app disclosures, explain what user data your app collects and transmits, how it's used, and the type of parties with whom it's shared. |
| Your app targets children | Your app must not include an SDK that is not approved for use in child-directed services. See Designing Apps for Children and Families for full policy language and requirements. |
| Your app collects or links persistent device identifiers (for example, IMEI, IMSI, SIM Serial #, etc.) | Persistent device identifiers may not be linked to other personal and sensitive user data or resettable device identifiers except for the purposes of<br>• Telephony linked to a SIM identity (for example, wifi calling linked to a carrier account), and<br>• Enterprise device management apps using device owner mode.<br>These uses must be prominently disclosed to users as specified in the User Data policy. |

| | |
|---|---|
| | Please consult this resource for alternative unique identifiers.<br>Please read the Ads policy for additional guidelines for Android Advertising ID. |

### Data safety section

All developers must complete a clear and accurate Data safety section for every app detailing collection, use, and sharing of user data. The developer is responsible for the accuracy of the label and keeping this information up-to-date. Where relevant, the section must be consistent with the disclosures made in the app's privacy policy.

Please refer to this article for additional information on completing the Data safety section.

### Privacy Policy

All apps must post a privacy policy link in the designated field within Play Console, and a privacy policy link or text within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app accesses, collects, uses, and shares user data, not limited by the data disclosed in the Data safety section. This must include:

- Developer information and a privacy point of contact or a mechanism to submit inquiries.
- Disclosing the types of personal and sensitive user data your app accesses, collects, uses, and shares; and any parties with which any personal or sensitive user data is shared.
- Secure data handling procedures for personal and sensitive user data.
- The developer's data retention and deletion policy.
- Clear labeling as a privacy policy (for example, listed as "privacy policy" in title).

The entity (for example, developer, company) named in the app's Google Play store listing must appear in the privacy policy or the app must be named in the privacy policy. Apps that do not access any personal and sensitive user data must still submit a privacy policy.

Please make sure your privacy policy is available on an active, publicly accessible and non-geofenced URL (no PDFs) and is non-editable.

### Account Deletion Requirement

If your app allows users to create an account from within your app, then it must also allow users to request for their account to be deleted. Users must have a readily discoverable option to initiate app account deletion from within your app and outside of your app (for example, by visiting your website). A link to this web resource must be entered in the designated URL form field within Play Console.

When you delete an app account based on a user's request, you must also delete the user data associated with that app account. Temporary account deactivation, disabling, or "freezing" the app account does not qualify as account deletion. If you need to retain certain data for legitimate reasons such as security, fraud prevention, or regulatory compliance, you must clearly inform users about your data retention practices (for example, within your privacy policy).

To learn more about account deletion policy requirements, please review this Help Center article. For additional information on updating your Data safety form, visit this article.

### Usage of App Set ID

Android will introduce a new ID to support essential use cases such as analytics and fraud prevention. Terms for the use of this ID are below.

- **Usage**: App set ID must not be used for ads personalization and ads measurement.
- **Association with personally-identifiable information or other identifiers:** App set ID may not be connected to any Android identifiers (for example, AAID) or any personal and sensitive data for advertising purposes.
- **Transparency and consent:** The collection and use of the app set ID and commitment to these terms must be disclosed to users in a legally adequate privacy notification, including your privacy policy. You must obtain users' legally valid consent where required. To learn more about our privacy standards, please review our User Data policy.

### EU-U.S., UK, and Swiss Data Privacy Frameworks

If you access, use, or process personal information made available by Google that directly or indirectly identifies an individual and that originated in the European Economic Area, United Kingdom, or Switzerland ("EU Personal Information"), then you must:

- Comply with all applicable privacy, data security, and data protection laws, directives, regulations, and rules;
- Access, use or process EU Personal Information only for purposes that are consistent with the consent obtained from the individual to whom the EU Personal Information relates;
- Implement appropriate organizational and technical measures to protect EU Personal Information against loss, misuse, and unauthorized or unlawful access, disclosure, alteration and destruction; and
- Provide the same level of protection as is required by the Data Privacy Framework Principles or the applicable transfer mechanism as described in the Google Controller-Controller Data Protection Terms.

You must monitor your compliance with these conditions on a regular basis. If, at any time, you cannot meet these conditions (or if there is a significant risk that you will not be able to meet them), you must immediately notify us by email to data-protection-office@google.com and immediately either stop processing EU Personal Information or take reasonable and appropriate steps to restore an adequate level of protection.

Help us improve this policy article by taking a **2-minute survey** .

Need more help?

Try these next steps:

**Post to the help community**
Get answers from community members

**Contact us**
Tell us more and we'll help you get there