Provide information for Google Play's Data safety section

Google Play's Data safety section provides developers with a transparent way to show users if and how they collect, share, and protect user data, before users install an app. Developers are required to tell us about their apps' privacy and security practices by completing a form in Play Console. This information is then shown on your app's store listing on Google Play.

This article provides an overview of the Data safety form requirements, guidance for completing the form, and information about any recent or upcoming changes.

COLLAPSE ALL EXPAND ALL

Overview

The Data safety section on Google Play is a simple way for you to help people understand what user data your app collects or shares, and to showcase your app's key privacy and security practices. This information helps users make more informed choices when deciding which apps to install.

All developers must declare how they collect and handle user data for the apps they publish on Google Play, and provide details about how they protect this data through security practices like encryption. This includes data collected and handled through any third-party libraries or SDKs used in their apps. You may want to refer to your SDK providers' published Data safety information for details. Check Google Play SDK Index to see if your provider has provided a link to their guidance.

You can provide this information through the Data safety form on the **App content** page (**Policy** > **App content)** in Play Console. After you complete and submit the Data safety form, Google Play reviews the information you provide as part of the app review process. It's then shown on your store listing to help Google Play users understand how you collect and share data before they download your app.

You alone are responsible for making complete and accurate declarations in your app's store listing on Google Play. Google Play reviews apps across all policy requirements; however we cannot make determinations on behalf of the developers of how they handle user data. Only you possess all the information required to complete the Data safety form. When Google becomes aware of a discrepancy between your app behavior and your declaration, we may take appropriate action, including enforcement action.

You can expand the section below to see how your store listing looks to Google Play users, and notifications and updates users may see if you make certain changes to your app's Data safety section.

What users will see if your app shares user data

What users will see if your app doesn't collect or share any user data

Which developers need to complete the Data safety form in Play Console?

All developers that have an app published on Google Play must complete the Data safety form, including apps on closed, open, or production testing tracks. This also applies to pregranted and preloaded apps that update through Google Play.

Tracks that are active on internal testing tracks are exempt from inclusion in the data safety section. Apps that are exclusively active on this track do not need to complete the Data safety form.

Even developers with apps that do not collect any user data must complete this form and provide a link to their privacy policy. In this case, the completed form and privacy policy can indicate that no user data is collected or shared.

System services and private apps do not need to complete the Data safety form.

While a global form is required for each app defined at the app package level, developers may exclude old artifacts from their form. This is applicable for artifacts with effective target SdkVersion below 21 where the majority of the app's active user install base (90%+) is on artifacts with effective target SdkVersion 21 or higher.

Getting your information ready

Before you provide information for Google Play's Data safety section, we recommend that you:

- Read and understand the requirements for completing the Data safety form in Play Console and complying with our User Data policy.
- Ensure that you've added a privacy policy; this is required to complete the Data safety form and have your data safety information shown to users.
- Review how your app collects and shares user data and your app's security practices. In particular, check your app's declared permissions and the APIs that your app uses.
- In addition to reviewing how your app collects and shares user data, you should also review how any third-party code (such as third-party libraries or SDKs) in your app collects and shares such data. It's your responsibility to ensure that any such code used in your app is compliant with Play Developer Program policies. You must reflect data collection or sharing carried out by such third-party code in the Data safety form for your app.
- Watch the Google Play PolicyBytes Data safety form walkthrough video below, which takes you through all the resources and steps required to complete the Data safety form.

Watch the Data safety form walkthrough video

What developers need to disclose in the Data safety form

This section explains what information you need to disclose in the Data safety form in Play Console, and lists the user data types and purposes you can select.

What developers need to declare across data types

Click on the sections below to expand or collapse them.

Data collection

Data sharing

Data handling

Other app and data disclosures

The Data safety section is also an opportunity for you to showcase your app's privacy and security practices to your users. For example, you can highlight the following information:

- **Encryption in transit:** Is data collected or shared by your app using encryption in transit to protect the flow of user data from the end user's device to the server.
  - Some apps are designed to let users transfer data to another site or service. For example, a messaging app may give users an option to send an SMS message through their mobile services provider, which maintains different encryption practices. These apps may declare in their Data safety section that data is transferred over a secure connection as long as they use best industry standards to safely encrypt data while it travels between a user's device and the app's servers.
- **Deletion request mechanism:** Does your app provide a way for users to request deletion of their data?

Committed to follow the Families policy (available March 2022 to applicable apps)

Independent security review (available to all apps)

Data types and purposes

Click on the sections below to expand or collapse them.

Data types

Developers will be asked to provide collection, sharing, and other practices for a range of user data types, as well as the purposes for which you use that data.

Category	Data type	Description
		User or device physical location to an area greater than or equal

Location	Approximate location	to 3 square kilometers, such as the city a user is in, or location provided by Android’s ACCESS_COARSE_LOCATION permission.
	Precise location	User or device physical location within an area less than 3 square kilometers, such as location provided by Android’s ACCESS_FINE_LOCATION permission.
Personal info	Name	How a user refers to themselves, such as their first or last name, or nickname.
	Email address	A user’s email address.
	User IDs	Identifiers that relate to an identifiable person. For example, an account ID, account number, or account name.
	Address	A user’s address, such as a mailing or home address.
	Phone number	A user’s phone number.
	Race and ethnicity	Information about a user’s race or ethnicity.
	Political or religious beliefs	Information about a user’s political or religious beliefs.
	Sexual orientation	Information about a user’s sexual orientation.
	Other info	Any other personal information such as date of birth, gender identity, veteran status, etc.
Financial info	User payment info	Information about a user’s financial accounts such as credit card number.
	Purchase history	Information about purchases or transactions a user has made.
	Credit score	Information about a user’s credit score.
	Other financial info	Any other financial information such as user salary or debts.
Health and fitness	Health info	Information about a user's health, such as medical records or symptoms.
	Fitness info	Information about a user's fitness, such as exercise or other physical activity.
Messages	Emails	A user’s emails including the email subject line, sender, recipients,

		and the content of the email.
	SMS or MMS	A user’s text messages including the sender, recipients, and the content of the message.
	Other in-app messages	Any other types of messages. For example, instant messages or chat content.
Photos and videos	Photos	A user’s photos.
	Videos	A user’s videos.
Audio files	Voice or sound recordings	A user’s voice such as a voicemail or a sound recording.
	Music files	A user’s music files.
	Other audio files	Any other user-created or user-provided audio files.
Files and docs	Files and docs	A user’s files or documents, or information about their files or documents such as file names.
Calendar	Calendar events	Information from a user’s calendar such as events, event notes, and attendees.
Contacts	Contacts	Information about the user’s contacts such as contact names, message history, and social graph information like usernames, contact recency, contact frequency, interaction duration and call history.
App activity	App interactions	Information about how a user interacts with the app. For example, the number of times they visit a page or sections they tap on.
	In-app search history	Information about what a user has searched for in your app.
	Installed apps	Information about the apps installed on a user's device.
	Other user-generated content	Any other user-generated content not listed here, or in any other section. For example, user bios, notes, or open-ended responses.
	Other actions	Any other user activity or actions in-app not listed here such as gameplay, likes, and dialog options.
Web browsing	Web browsing	Information about the websites a user has visited.

	history	
App info and performance	Crash logs	Crash log data from your app. For example, the number of times your app has crashed, stack traces, or other information directly related to a crash.
	Diagnostics	Information about the performance of your app. For example battery life, loading time, latency, framerate, or any technical diagnostics.
	Other app performance data	Any other app performance data not listed here.
Device or other IDs	Device or other IDs	Identifiers that relate to an individual device, browser or app. For example, an IMEI number, MAC address, Widevine Device ID, Firebase installation ID, or advertising identifier.

Purposes

Completing the Data safety form in Play Console

You can tell us about your app's privacy and security practices in the Data safety form on the **App content** page in Play Console.

Overview

First, you'll be asked whether your app collects or shares certain types of user data. This is where you let us know whether your app collects or shares any of the required user data types. If it does, you'll be asked some questions about your privacy and security practices. If you're unsure about any of these questions, you can save your form as a draft at any time and return to it later.

Next, you'll answer some questions about each type of user data. If your app does collect or share any of the required user data types, you'll be asked to select them. For each type of data, you'll be asked questions about how the data is used and handled.

Before you submit, you'll see a preview of what will be shown to users on your store listing. After you submit, the information you provided will be reviewed by Google as part of the app review process.

Google's review process is not designed to verify the accuracy and completeness of your data safety declarations. While we may detect certain discrepancies in your declarations and we will be taking appropriate enforcement measures when we do, only you possess all the information required to complete the Data safety form. You alone are responsible for making complete and accurate declarations in your app's store listing on Google Play.

Complete and submit your form

When you're ready to start, here's how you complete and submit your Data safety form in Play

Console:

1. Open Play Console and go to the App content page (**Policy** > **App content**).
2. Under "Data safety," select **Start**.
3. Before you start the form, read the "Overview" section. This provides information about the questions you'll be asked, and the information you'll need to provide. When you've finished reading and are ready to get started, select **Next** to move on to the next section.
4. In the "Data collection and security" section, review the list of required user data types that you need to disclose. If your app collects or shares any of the required user data types, select **Yes**. If not, select **No**.
5. If you selected Yes, confirm the following by answering **Yes** or **No**:
   - Whether or not all of the user data collected by your app is encrypted in transit.
   - Whether or not you provide a way for users to request that their data is deleted.
6. Select **Next** to move on to the next section.
7. In the "Data types" section, select all of the user data types collected or shared by your app. When you're finished, select **Next** to move on to the next section. You must [complete this section in accordance with the data collection and sharing guidance above.
8. In the "Data usage and handling" section, answer questions about how the data is used and handled for each user data type your app collects or shares. Next to each user data type, select **Start** to answer the questions. When you're finished, select **Next** to move on to the next section.
   - **Note:** You can change the user data types that are selected by going back to the previous section and changing your selections.
9. After answering all questions, the "Store listing preview" section previews the information that will be shown to users on Google Play based on the form answers you've provided. Review this information.

If you're ready to submit your completed form, select **Submit**. If you want to go back and change something, you can select **Back** to amend your answers. If you're not sure about something, you can select **Save as draft** and return to the form later. If you select **Discard changes**, you'll need to start the form again.

Import or export your form responses

You can export your form responses to a CSV file. You can also download a sample CSV, complete the form offline, and import your completed form from the CSV.

Click here to download a sample CSV .

Understand the CSV format

Export to a CSV file

Import from a CSV file

After you submit your Data safety form

After you submit, the information you provided will be reviewed by Google as part of the app review process.

Until July 20, 2022, you can temporarily proceed to publish app updates regardless of whether we find issues with the information you've disclosed. If there are no issues, your app will be approved and you won't need to do anything. If there are issues, you will need to revert your Data safety form's status to "Draft" in Play Console to publish your app update. We will also send the developer account owner an email, an Inbox message in Play Console, and show this information on the **Policy status** (**Policy** > **Policy status**) page.

After July 20, 2022, all apps will be required to have completed an accurate Data safety form that discloses their data collection and sharing practices (including apps that do not collect any user data).

Optional format for SDKs

If you're an SDK provider, you can click on the section below to view an optional format you can use to publish guidance for your users.

Developers will need to disclose their app's data collection, sharing, and security practices as part of Google Play's new Data safety section. To assist developers in helping build user data and security transparency, the guidance below can be used to publish SDK guidance for developers incorporating your SDK into their apps.

Google Play is publishing this optional structure for SDK developers to use at your convenience, but you may use any format or none based on the needs of your users.

Optional format for SDKs

Frequently asked questions

COLLAPSE ALL EXPAND ALL

App submission and review

What if I need additional time to comply with the new requirements?

Can my app be blocked by Google Play due to the information I submit in my Data safety form?

How long does it take for Data safety updates made through Play Console to show on Google Play?

What can I do to troubleshoot if I'm not seeing my Data safety section published?

I submitted similar information for iOS. How much of that work can I re-use for the Data safety form?

How do you make sure developers share accurate information? We've seen that this information is not always accurate in the industry.

Does Google regulate if the data that I collect is ultimately appropriate?

How often do I need to update my Data safety section?

Can the Data safety section on Google Play impact app downloads?

Completing the Data safety form

What if my app behaves differently in different supported Android versions?

How can I show that we may have different practices in different regions? For example, we don't use certain libraries in Europe, but we may use them in others.

Are the Data safety sections gated by a consent mechanism for users? Do I need to take any extra steps and create an in-app prominent disclosure?

How should I mark required or optional collection when different versions of my app that show a Data safety section do different things?

Do I need to declare data if my app includes a permission but does not actually collect or share the data?

If one data type is collected as part of another, should I declare both? For example, if I collected Contacts which includes the user's email, do I declare both the "Contacts" and "Email address" data types?

Am I required to provide a deletion mechanism? Must it be for any and all user data?

Is there a specific type of mechanism that I must provide to indicate my app supports user data deletion requests?

How should I indicate in my Data safety form that I provide a request for deletion mechanism for data that is automatically deleted or anonymized?

What if the deletion mechanism I provide is not available globally to all users — can I still indicate I provide a deletion request mechanism?

What kinds of techniques can be used to make data anonymous?

How should I treat the collection and use of IP addresses?

How should I disclose the collection and sharing of other kinds of identifiers?

What kinds of activities can "service providers" perform?

My app uses an external payment service to enable financial transactions. Does my app need to disclose financial information like credit card info in its Data safety section?

My app enables users to upload their data directly to Google Drive or Dropbox for backup or storage. My app does not access any of this data. Should that still be disclosed as "collection"?

How should I encrypt data in transit?

My app lets the user create an account or add information to their account, for example, birthday or gender. How should I declare the data that the user adds to their account?

What are System services?

My app's Data safety section submission was approved but I recently received a notification regarding an update. How do I check the current status of my submission and is that not permanent?

How do I declare collection of data that is used in a transient way to load pages and service other client-side requests in real time before that data is logged on our servers and used for other purposes?

What is the difference between the permissions list and the Data safety section of an app?

Change log

You can refer to this section to see a revision history for this article, so you can keep track of changes over time. We'll add dated entries here whenever we make significant changes to this article in the future.

March 31, 2023

August 24, 2022

July 20, 2022

June 28, 2022

April 26, 2022

April 8, 2022

February 24, 2022

December 14, 2021

Other resources

- Learn more about reviewing how your app collects and shares user data on the Android Developers site .
- Learn more about best practices and review the interactive guidance on the Academy for App Success .

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in