M Gmail

Action Required: Your app is not compliant with Google Play Policies (DSM-Absen)

2 pesan

Google Play Support <no-reply-googleplay-developer@google.com>   2 April 2023 pukul 07.57
Balas Ke: Google Play Support <no-reply-googleplay-developer@google.com>
Kepada: cv.rebahanberdikari@gmail.com
Cc: cv.rebahanberdikari@gmail.com

Google Play   Developer update

Hi Developers at Generasi Rebahan Berdikari,

After a recent review, we found that your app DSM-Absen (com.infinity.dsmabsen) is not compliant with one or more of our Developer Program Policies. See below for more information about your app's status and how to correct the issue.

⚠️	App Status: Rejected Your app has been rejected and wasn't published due to the policy issue(s) listed below. If you submitted an update, the previous version of your app is still available on Google Play.
🔧	Issue found: Not a core feature The app feature that you declared as dependent on the All files access permission didn't meet the policy review requirements for critical core functionality. Core functionality is defined as the main purpose of the app. Without this core functionality, the app is "broken" or rendered unusable. The core functionality, as well as any core features that comprise this core functionality, must all be prominently documented and promoted in your app's store listing description on Google Play. Update your app so that the feature doesn't use this permission. If your app doesn't require access to the MANAGE_EXTERNAL_STORAGE permission, you must remove it from your app's manifest in order to successfully meet the policy review requirements. Alternatively, if your app is "broken" or rendered unusable without this permission, it's likely your earlier declaration was misstated or is

unclear. Ensure that the core functionality and technical justification are clearly documented and promoted in the app's description when you complete the Permissions Declaration Form, and resubmit your app on the Play Console.

Additionally, follow these steps to bring your app into compliance:

Follow these steps to bring your app into compliance:

- Review the All Files Access Permission policy.
- Read more about Use of All files access permission to better understand permitted and invalid uses.
- Review Android storage use cases and best practices for common storage use cases.
- If your app meets the requirements of permitted uses, read how to Declare permissions for your app.

About the All Files Access Permission policy

Files and directory attributes on a user's device are regarded as personal and sensitive user data subject to the Personal and Sensitive Information policy and the following requirements:

- Apps should only request access to device storage which is critical for the app to function, and may not request access to device storage on behalf of any third-party for any purpose that is unrelated to critical user-facing app functionality.
- Android devices running Android "R" (Android 11) or later, will require the MANAGE_EXTERNAL_STORAGE permission in order to manage access to shared storage. All apps that target R or later and request broad access to shared storage ("All files access") must successfully pass an appropriate access review prior to publishing. Apps allowed to use this permission must clearly prompt users to enable "All files access" for their app under "Special app access" settings. For more information on the R requirements, see Use of All files access (MANAGE_EXTERNAL_STORAGE) permission.

Issue found: Need to use MediaStore API or No Access to Files

You requested access to All files access permission but it appears that your app's core feature requires access to only Media Files or doesn't need access to any files. In either case, you need to remove All files access permission since access to all files isn't critical to your app's core functionality.

If users needs access and store Media Files only, you should use the MediaStore API. This API permits your app to contribute to and access media that's available on an external storage volume without the need for the All files access permission.

Update your app so that the feature uses MediaStore APIs and remove All files access (MANAGE_EXTERNAL_STORAGE) permission.

Additionally, follow these steps to bring your app into compliance:

- Make sure to read the applicable or requirements listed:
- Review the All Files Access Permission policy.
- Read more about Use of All files access permission to better understand permitted and invalid uses.
- See Android storage use cases and best practices for common storage use cases.
- Review how to Access media files from shared storage to see how you can access the media store.

About the All Files Access Permission policy

Files and directory attributes on a user's device are regarded as personal and sensitive user data subject to the Personal and Sensitive Information policy and the following requirements:

- Apps should only request access to device storage which is critical for the app to function, and may not request access to device storage on behalf of any third-party for any purpose that is unrelated to critical user-facing app functionality.
- Android devices running Android "R" (Android 11) or later, will require the MANAGE_EXTERNAL_STORAGE permission in order to manage access to shared storage. All apps that target R or later and request broad access to shared storage ("All files access") must successfully pass an appropriate access review prior to publishing. Apps allowed to use this permission must clearly prompt users to enable "All files access" for their app under "Special app access" settings. For more information on the R requirements, see Use of All files access (MANAGE_EXTERNAL_STORAGE) permission.

Action required: Submit an updated app for review

Here's what to do to help get your app on Google Play:

1. Make sure to read the applicable policies or requirements listed below:
   - All Files Access Permission policy
2. Make appropriate changes to your app (if possible), and be sure to address the issue described above. You may also want to check your app's store listing for compliance, if applicable.
3. Double check that your app is compliant with all other Developer Program Policies.
4. If you made changes to your app bundle, store listing, or APK, please sign in to your Play Console and submit the update(s).

Contact support

If you've reviewed the policy and feel our decision may have been in error, please reach out to our policy support team. We'll get back to you within 2 business days.

Learn More

Visit the Android Developers Blog to learn more about free tools and resources for building safe and successful apps.

Thanks for your continued support in helping to make Google Play a positive experience for both developers and consumers. We look forward to seeing an updated version of your app on Google Play.

Please complete a two question survey to help us improve this experience.

The Google Play Team

Learn more about Google Play policy

Get started on Play Academy

© 2023 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043

Click here to configure your notification preferences.

This message was sent to inform you about important updates to your Google Play developer account.

Google Play Support <no-reply-googleplay-developer@google.com>   2 April 2023 pukul 07.57
Balas Ke: Google Play Support <no-reply-googleplay-developer@google.com>
Kepada: cv.rebahanberdikari@gmail.com
Cc: cv.rebahanberdikari@gmail.com

Google Play   Developer update

Hi Developers at Generasi Rebahan Berdikari,

After a recent review, we found that your app DSM-Absen (com.infinity.dsmabsen) is not compliant with one or more of our Developer Program Policies. See below for more information about your app's status and how to correct the issue.

⚠️	**App Status: Rejected** Your app has been rejected and wasn't published due to the policy issue(s) listed below. If you submitted an update, the previous version of your app is still available on Google Play.
🔧	Issue found: Invalid Data safety form We reviewed your app's Data safety form in Play Console and found discrepancies between it and how the app collects and shares user data. All apps are required to complete an accurate Data safety form that discloses their data collection and sharing practices - this is required even if your app does not collect any user data.

We detected user data transmitted off device that you have not disclosed in your app's Data safety form as user data collected.

You must ensure that your app's Data safety section accurately reflects your app's data collection, sharing, and handling practices. This includes data collected and handled through any third-party libraries or SDKs used in your app. When available, we've included details on SDKs that contain code similar to the code in your APK that may be sending user data off device. You can check if your app uses any of these SDKs, but note that this list of SDKs may not be exhaustive. You must review and account for all data collected and shared by your app.

Issue details

We found an issue in the following area(s):

- **SPLIT_BUNDLE 2: Policy Declaration - Data Safety Section**: Device Or Other IDs Data Type - Device Or Other IDs (some common examples may include Advertising ID, Android ID, IMEI, BSSID, MAC address)

About the Data safety section in Google Play User Data policy

Your app must be in compliance with this policy. If your app continues to be non-compliant, your app updates will be rejected and your app may face additional enforcement actions in the future.

Please make changes to align your app's Data safety form with the app's behavior. This can be done by either:

- Updating your form in Play Console to declare collection of Data Types noted below; or
- Removing unwanted functionality and attributable code that collects this user data from your app or libraries used in your app, and when applicable to deactivate all non-compliant APKs.
    - To deactivate non-compliant APKS, you can create a new release and upload a compliant APK to each track containing the non-compliant APKs.
    - Be sure to increment the APK version code. If using staged rollout, be sure to set the release to 100% rollout.

For helpful resources, you can:

- Learn more about how to provide app privacy and security information for Google Play's Data safety section.
- Watch the Google Play PolicyBytes - Data safety form walkthrough.
- Check Google Play SDK Index to see if your SDK provider has shared a link to their data safety guidance. Review how any third-party code (such as third-party libraries or SDKs) in your app collects and shares user data.

Action required: Submit an updated app for review

Here's what to do to help get your app on Google Play:

1. Make sure to read the applicable policies or requirements listed below:
    - Data safety section in Google Play User Data policy

2. Make appropriate changes to your app (if possible), and be sure to address the issue described above. You may also want to check your app's store listing for compliance, if applicable.
3. Double check that your app is compliant with all other Developer Program Policies.
4. If you made changes to your app bundle, store listing, or APK, please sign in to your Play Console and submit the update(s).

Contact support

If you've reviewed the policy and feel our decision may have been in error, please reach out to our policy support team. We'll get back to you within 2 business days.

Learn More

Visit the Android Developers Blog to learn more about free tools and resources for building safe and successful apps.

Thanks for your continued support in helping to make Google Play a positive experience for both developers and consumers. We look forward to seeing an updated version of your app on Google Play.

Please complete a two question survey to help us improve this experience.

The Google Play Team

Learn more about Google Play policy

Get started on Play Academy