

Action Required: Your app is not compliant with Google Play Policies (AI Writing Assistant - NexBot)

- Google Play Support <no-reply-googleplay-developer@google.com>
- <ciphre.bytes@gmail.com>

Google Play Support

Wednesday, November 8th 2023, 3:49:30 PM PST

To: ciphre.bytes@gmail.com (Me), admin



Developer update

Hi Developers at Stackwares,

After a recent review, we found that your app AI Writing Assistant - NexBot (com.nexbot.app) 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: Violation of User Data, Permissions and APIs that Access Sensitive Information Policies

We have observed that your app is using an SDK that is designed to collect device location by default. This SDK can result in your app violating the prominent disclosure and consent and/or approved purpose requirements of Google Play's User Data and Permissions and APIs that Access Sensitive Information policies. You are hereby requested to provide evidence of your compliance with the Prominent Disclosure and Consent requirements. Your app submissions will be rejected pending your action.

Issue details

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

- **Version code 42:**
 - SDK: MyTarget com.my.target:mytarget-sdk

To bring your app into compliance, follow these steps:

Verify that your app accesses, collects, uses, and shares (including with SDKs) device location only for approved purposes and in compliance with the applicable prominent disclosure and consent requirements of the above-mentioned policies. Do not enable SDK data collection if it violates these requirements.

Submit an appeal of this rejection and attach evidence (e.g. screenshots or a video demonstration of the in-app prominent disclosure and consent experience) of your compliance with the Prominent Disclosure requirements.

In the alternative, you may consider removing the SDK code designed to collect personal and sensitive user data by default, or moving to an alternative SDK or version which includes the appropriate technical mechanism to ensure that end user consent information collected by apps is honored. You may consider upgrading to a policy-compliant version of this SDK, if available from your SDK provider or removing the SDK. Google is unable to endorse or recommend any third party software.

- MyTarget com.my.target:mytarget-sdk: Consider upgrading to a policy-compliant version of the SDK if available from your SDK provider, or removing the SDK.

About the User Data policy

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. If your app handles sensitive user data, then you must follow the Personal and Sensitive User Data policy.

According to Personal and Sensitive User Data policy, 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.

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, microphone, camera, and other sensitive device or usage data.

About the Permissions and APIs that Access Sensitive Information policy

Request permissions and APIs that access sensitive information to access data in context (via incremental requests), so that users understand why your app is requesting the permission. Use the data only for purposes that the

user has consented to. If you later wish to use the data for other purposes, you must ask users and make sure they affirmatively agree to the additional uses.

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:
 - o User Data policy
 - o Permissions and APIs that Access Sensitive Information 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. Check out the latest Google Play policy updates on Full Screen Intent Permission, Health Apps, Photo and Video Permissions, AI-Generated Content, and more! Watch now: #PolicyBytes

Thanks for your continued support in helping to make Google Play a positive experience for both developers and consumers.

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.

