If you dont see this email click here

Complying with the Google Play User Data Policy

29/3/2017

In February of this year, a number of tech websites reported that Google had sent messages to the owners of apps offered on Google Play threatening to remove the apps from Google Play on the grounds that Google's privacy requirements were being violated.

Google did not make a public statement about an intention to remove violating apps. If an app owner has not received a warning message from Google, it does not appear that they are in immediate danger of being removed. Nevertheless, under the terms of the Google Play Developer Distribution Agreement, Google may reclassify an app or remove an app altogether from the Google Play store in case of violations of the terms of the Distribution Agreement and Google's Developer Program Policies. In addition, Google can require the app owner to refund payments received for downloads in the last year. Therefore, even if you have not received a warning message from Google, we recommend that you comply with the privacy requirements contained in the User Data policy which forms part of the Developer Program Policies. This can be found in the Developer Policy Center.

According to the User Data policy:

"You must be transparent in how you handle user data (e.g., information provided by a user, collected about a user, and collected about a user's use of the app or device), including by disclosing the collection, use, and sharing of the data, and you must limit use of the data to the description in the disclosure. If your app handles personal or sensitive user data, there are additional requirements described below."

The User Data policy goes on to define personal or sensitive data as "*including personally identifiable information, financial and payment information, authentication information, phonebook or contact data, microphone and camera sensor data, and sensitive device data*." Note that under EU law, even an IP address may be considered personally identifiable information. If your app requests permissions to access this kind of data, including use of contacts/phonebook, the phone itself, the camera or microphone, or accounts, it may also be considered by Google to fall into this category. Remember, this is not only about data that you collect and store, but data which your app "handles."

Recommendations:

In light of the above, we would advise our clients to do the following:

1. Create a Privacy Policy if You Don't Have One. In order to comply with Google's requirements and applicable law, and even if Google would not deem the data handled by your app to be "*personal or sensitive data*" we recommend that you maintain a Privacy Policy, which informs users what data you receive, collect or share when the app is downloaded and used. It is important to say what is done with the data.

2. Review Existing Privacy Policy. If you already have a Privacy Policy, we recommend reviewing and updating it periodically to make sure that it reflects your current data practices.

3. Requirements for Handling Personal/Sensitive Data. If your app does collect personal or sensitive data, Google requires that your Privacy Policy "*comprehensively disclose how your app collects, uses and shares user data, including the types of parties with whom it's shared*" and that you "*handle the user data securely, including transmitting it using modern cryptography (for example, over HTTPS)."*

4. Where to Post Your Privacy Policy. In addition, and this was the problem specified in the reported warning messages from Google, you must post your privacy policy "*in both the designated field in the Play Developer Console and from within the Play distributed app itself."* Again, we recommend doing both of these in all cases.

   Even if the content of your privacy policy meets all legal (and Google) requirements, if the only place to find it is by separately visiting your website, users will not have been given a chance to review the Privacy Policy before or even while they use the app, defeating the purpose of having a

Privacy Policy and possibly depriving you of the benefits under applicable law. In the Google Play Developer Console you should be able to enter a URL to the Privacy Policy after selecting the app and then Store Listing.

5. Prominent Highlighting Required for Certain Data. The User Data policy provides heightened requirements where the personal or sensitive data handled by the app is "*unrelated to functionality described prominently in the app's listing on Google Play or in the app interface.*" In such a case, before obtaining and transmitting the user data, the app "*must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.*"

A Final Word: Please note that Google is not the only app platform which maintains privacy and other requirements which your app must meet. Apple imposes requirements on apps in the iTunes App Store, and Facebook maintains developer policies which apply to both Facebook apps (which may include plug-in functionality you add to your website) and chat bots. The law of the jurisdiction in which your app is offered may also have other requirements.

If you need assistance in creating or updating a Privacy Policy for your app (or website or other online product or service), and complying with the Google's User Data policy or other requirements mandated by Google, or other entities like Apple and Facebook, feel free to contact us.

Contact Person

David Mirchin, Partner, Technology, IP and Data Protection

Tel: +972-3-6103199
Mail: dmirchin@meitar.com

More Information

For more information about Meitar's Technology and Intellectual Property group, click here