Google Mandates Play Store and In-App Privacy Policies

Article
March 28, 2017

Google updated its Google Play Developer Policy Center policies on March 1, 2017, and the updates went into effect on March 15, 2017. These updates included requirements for developers to post privacy policies both on the Play Store listing and within the app.

According to Google, app developers "must be transparent in how [apps] handle user data." If an app stores personal or sensitive user data (i) provided by a user, (ii) collected about a user or (iii) collected about a user's use of an app or device, then the developer must post a privacy policy in both the Play Store and the app itself.

Google provides several examples of "personal or sensitive" user data that trigger the privacy policy mandate, including personally identifiable information, financial and payment information, authentication information, phonebook or contact data, microphone and camera sensor data and sensitive device data. Responsive privacy policies must "comprehensively disclose" how the app collects, uses and shares user data and the types of parties with whom data is shared. Additionally, all information used by the app must be handled securely and transmitted with modern cryptography, such as HTTPS.

Certain types of data have more additional requirements:

- apps that collect personal or sensitive user data that is unrelated to the app's function listed in the Play Store or the application's interface must prominently highlight how that user data will be used and obtain affirmative consent from the user for such use;
- apps that handle financial or payment information "must never publicly disclose and personal or sensitive user data related to financial or payment activities;" and
- no app is permitted to publish or disclose a user's non-public phonebook or contact information.

Google provided specific examples of common privacy and security violations. For example, an app that fails to handle a user's inventory of installed apps or phonebook information as personal or sensitive user data violates the Privacy Policy, Secure Transmission and Prominent Disclosure requirements.

PROFESSIONALS

Christopher J. Jaekels
Partner

RELATED SERVICES

Corporate & Securities

Finally, apps that monitor or track a user's behavior must:

- not be presented or described as a means for spying or secret surveillance;
- not hide or cloak tracking behavior;
- present users with a persistent notification and unique icon that clearly identifies the app; and
- not provide any means to activate or access functionality that would violate Google's Developer Policy Center policies (for example, an app cannot link to a non-compliant Android Package Kit, or APK, hosted outside the Play Store).

Developers should make sure that they read and review Google's updated privacy and security requirements. Apps that are currently not in compliance risk being removed from the Play Store. Additionally, developers should ensure that their apps comply with state and federal laws on the handling and disclosure of private and sensitive information.