Nueva sección de privacidad de la Google Play Store: Data Safety

Por: Diego Morabito. 11/08/2022

- La Google Play Store eliminó la lista de permisos para aplicaciones y agregó una nueva sección con información sobre seguridad y privacidad “Data Safety”
- Con esta nueva sección, Google deja en manos de quienes desarrollan las apps, informar a las personas usuarias sobre que datos recolectan las apps y cómo los utiliza
- Este nuevo cambio será obligatorio para todas las aplicaciones de Google Play Store a partir del 20 de julio

A finales de abril de 2022 Google implementó un nuevo modelo de información sobre el tratamiento de datos en su Play Store. Antes, la información disponible sobre el manejo de datos de las personas usuarias era básicamente: la política de privacidad y el despliegue de los permisos de acceso: fotos, video, internet, contacto. etc.

Sabemos que muchas de estas políticas de privacidad son largas, complejas y ambiguas respecto a cómo recopilan y manejan los datos de millones de usuarios.

Ahora, con esta nueva implementación, Google apunta a brindar más información pidiendo a quienes desarrollan las aplicaciones compartir qué datos recolectan y por qué, así las personas usuarias pueden descargar la app con conocimiento de esta información.

¿Cuáles son los cambios en la PlayStore?

1. Desarrolladores declaran información a la PlayStore.

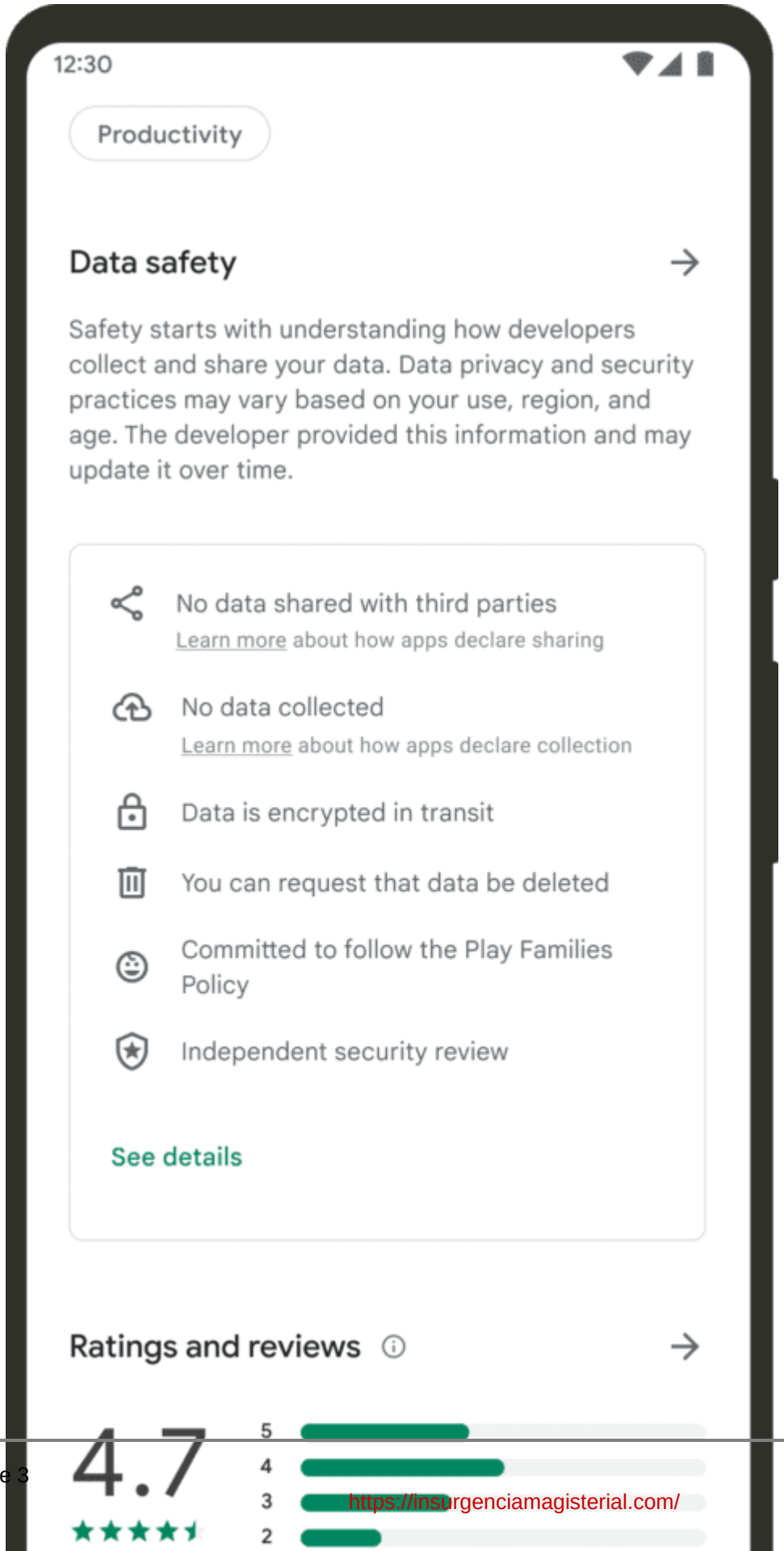
Las y los desarrolladores que tengan una aplicación publicada en la PlayStore tienen hasta **julio de 2022** para rellenar un formulario con información sobre el uso y recolección que le dan a los datos de las personas usuarias. Aquí puedes leer el

comunicado de Google.

Hay que tener en cuenta que quienes desarrollan son responsables de revelar el tratamiento de los datos. Y que a partir del **20 de julio**, ningún desarrollador puede publicar nuevas aplicaciones o actualizarlas si no ha llenado el formulario. Google señala que si identifica discrepancias entre lo que afirma quien desarrolla y el comportamiento real de la aplicación, se reserva el derecho a tomar las medidas apropiadas (no especifica estas medidas).

El comunicado tampoco especifica el proceso de revisión, si es un proceso de revisión automatizado, con un equipo humano o mixto.

2. Nueva información desplegada en la PlayStore:


12:30
Productivity
Data safety
Safety starts with understanding how developers collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this information and may update it over time.
No data shared with third parties
Learn more about how apps declare sharing
No data collected
Learn more about how apps declare collection
Data is encrypted in transit
You can request that data be deleted
Committed to follow the Play Families Policy
Independent security review
See details
Ratings and reviews
4.7
5
4
3
2

Aquí detallamos la información que deben publicar quienes desarrollan aplicaciones y la información que no es obligatoria:

2.1 Recolección de datos. Se refiere a todos aquellos datos que son recopilados y enviados a servidores externos. Estos datos incluyen:

- Los datos que son extraídos y generados mediante librerías y *sdk*'s.
- Datos generados en *Webview* que sea controlada por el desarrollador.
- Datos que fácilmente pueden ser asociados con un usuario, es decir, que pueden permitir la asociación con la persona física.

Sobre la **recolección de datos**, este otro tipo de información no es obligatoria, por lo que no aparecerá en la Play Store:

- Datos que son usados de manera efímera (que sólo están en la memoria por cierto tiempo para cumplir una función particular).
- Datos cifrados de punto a punto donde sólo los usuarios tengan acceso a esos datos (como los mensajes de Whatsapp).

Cuando se compartan los datos con personas morales o físicas, quienes desarrollan deben reportar:

2.2 Datos compartidos con terceros.

- Todos aquellos datos generados por librerías y *sdk*'s que son compartidos con un tercero.
- Los datos compartidos con otra aplicación que esté en el mismo dispositivo.
- Datos generados en *Webview* que son compartidos con un tercero, siempre y cuando el desarrollador esté en control de la página web.

Sobre los **datos compartidos con terceros**, esta información no se considera obligatoria:

- Cuando el tercero le está ofreciendo un servicio al desarrollador, de tal manera que legalmente el desarrollador es responsable por el uso de esos datos.
- Datos compartidos para fines legales o por solicitudes del gobierno.
- Datos que el usuario sabe que serán compartidos y que conscientemente

accede a ello.
- Datos completamente anonimizados.

2.3 Aspectos de recolección y tipos de datos. Quienes desarrollan deben especificar los siguientes puntos:

- Si los datos requeridos son opcionales u obligatorios.
- El tipo de datos recolectados (ubicación, información personal, contactos, cámara y fotos, etc.)
- Razones de uso de los datos (Funcionalidad de la aplicación, Analítica, Marketing, etc.).

2.4 Prácticas de seguridad. Agregar la siguiente información es opcional.

- En la sección “Seguridad de los datos” (*Data Safety*), especificar si la aplicación cuenta con mecanismos de seguridad (HTTPS, por ejemplo), para la transferencia de datos entre la aplicación y los servidores.
- Especificar si existe la posibilidad de que la persona usuaria pueda solicitar que sus datos sean borrados.
- Especificar si la seguridad de su aplicación fue validada por Laboratorios de Seguridad avalados por Google.

Aquí pueden consultar las políticas de privacidad que deben seguir las y los desarrolladores de aplicaciones: Link 1, 2. Además el link a la explicación de cómo se recopilan ciertos datos y la definición de cierto tipo de datos.

Observaciones:

1. ¿Los datos anónimos se mantienen anónimos?

Es importante entender las distinciones que hace Google sobre los datos. Afirma que se debe reportar como **recolección de datos** todo aquello que se adquiere por medio de *sdk*’s y librerías de código. También se reporta como **datos compartidos con terceros** todos aquellos datos que no son anónimos, pero en caso de que sí lo sean, entonces no es necesario reportarlo. Es decir, como desarrollador/a debo informar como **recolección de datos** los metadatos extraídos por *trackers* (que son un buen ejemplo de un *sdk*), pero como éstos son anónimos (o fueron anonimizados), no es necesario divulgar si estos son **datos que se comparten con terceros**

.

El problema de lo anterior radica en que gran parte del ecosistema de extractivismo de datos sobrevive con este tipo de datos anónimos, y justo porque son anónimos, la discusión sobre la privacidad de las personas usuarias toma una forma velada.

Si los datos que Google, Facebook, Microsoft, y los grandes *data brokers* como Verisk, Acxiom y Oracle obtienen de una persona son anónimos o fueron anonimizados, entonces ¿su privacidad nunca fue violada?

La manera en la que Google reconoce los datos es sintomática del uso que le dan y el negocio que hacen con ellos. Además, si se tiene información adicional sobre una persona usuaria (cada dato distinto de un usuario se llama *data point*) es posible de-anonimizar la información que, nos dice Google, es anónima. Aquí el link a una historia publicada por Ars Technica.

2. ¿Quiénes son los terceros?

Por otro lado, es importante señalar que no se especifica quiénes son esos terceros con los que se comparten los datos, ni hay claridad sobre porqué se comparten datos con ellos ni en qué términos. Las categorías: de **Análisis** o **Marketing**, son ambiguas. ¿Qué están analizando? ¿Para qué? ¿Cómo? y por el lado de marketing, ¿cómo usan esos datos? Las personas usuarias tenemos derecho a saber si estos datos son, por ejemplo, una forma, por parte de los desarrolladores para monetizar la aplicación y qué hacen esos terceros anónimos con esos datos.

3. ¿Y los datos compartidos con gobiernos?

Asimismo, es preocupante que no sea obligatorio explicar si se comparten datos con el gobierno (y cuál gobierno). Siendo éste el organismo que legalmente puede ejercer la fuerza, muchos datos de las personas usuarias pueden ser utilizados de forma abusiva, ya sea en regímenes democráticos o totalitarios.

Si bien es cierto que explicitar, como ahora lo hace Google, toda esta información sobre el uso de y tratamiento de datos en las aplicaciones es un buen paso hacia el camino correcto de la privacidad y la elección informada de las personas usuarias, hace falta detalle y contexto de cierta información.

4. ¿Y la lista de permisos que piden las aplicaciones?

Nos gustaría agregar que no está claro por qué dejó Google de listar los permisos que requiere una aplicación. Esa información es relevante para la privacidad y seguridad.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: BR Atsit

Fecha de creación
2022/08/11