AppGuard Privacy Policy

Last Updated: June 9, 2023

We believe that you should always know what kind of data we collect from you, how we collect it, and how you can have control over your data. We strive to be transparent in our data collection efforts and to provide you with the information that you need to make decisions about our collection of data from you. This is the purpose of our privacy policy. There are certain things that you should be aware of when using our mobile application. Anything that you do on the AppGuard mobile application is tied to your account, which is automatically created when you use the mobile application. When you use the AppGuard mobile application, even if you are just browsing, we may collect some basic technical data from you such as the type of mobile device that you are using, your geographical location, and your IP address. When you use the mobile application, a user account is automatically created for you and requires you to share additional data with us, which is outlined below. We also provide you with the ability to limit the data that we collect from you and how we use it. If you have any questions about our privacy policy, how we collect data from you, how we use your data, or how you can control your privacy settings, you can contact us at any time at support@AppGuard.co.

Data You Share With Us

We may collect data from you when you voluntarily share it with us. This may include the following data:

- Account Data. An account is automatically created for you when you use the AppGuard mobile application. This account is tied to your device ID.
- Private Communication Data. We may use your contact data, such as any data that you voluntarily provide to us like your phone number, email address, social media account handles, contacts, or communications, to authenticate your account, to communicate with you, to respond to communications sent to you by us, to keep records of our communication, or to pursue or defend against legal claims. We may store and process your private communication data to scan for malicious content, to review content for violations of our terms of use agreement, or to respond to legal process or law enforcement inquiries.
- Sensitive Personal Information (as defined by California law and the GDPR). Sensitive personal information includes personal information such as account log-ins, passwords, or other credentials, text messages, or biometric data. We do not collect sensitive personal information when you use the AppGuard mobile application.

Additional Data We Receive From You

We may also collect data from you automatically when you use the AppGuard mobile application. This may include the following data:

- Location Data. We may collect data about your location by collecting and processing your IP address and device settings. We may use this data to provide location-based services, tailor our services to your geographic location, respond to law enforcement requests, or to provide you with advertisements or content that is relevant to your geographic location.

- Technical Data. We may collect technical data about your use of the AppGuard mobile application, such as your IP address, your device IDs, your screen resolution, the mobile application's bundle ID, the ad or creative ID, your mobile phone model, mobile carrier, your operating system, your geolocation, and your time zone. We may use this data to analyze your use of the AppGuard mobile application, to detect ad fraud or fraudulent impressions, to administer and secure our services, to determine how AppGuard should allocate resources to its mobile application, and to understand any technical load on AppGuard servers.
- Usage and Interaction Data. We may collect usage and interaction data from you when you use the AppGuard application, such as logs of user actions within the AppGuard mobile application or of the manner in which you interact with AppGuard mobile application. We may use this data to better tailor our services or to understand how we can improve our graphical user interfaces, which may include our remote configuration of the user interface of our mobile application to improve its functionality.
- Marketing Data. As a free service, we rely on advertisements to generate revenue to fund the AppGuard mobile application. We may collect your IP address, your application bundle ID, your advertising or creative ID, your device IDs, your geographical location, your pages visited, referring web page, mobile phone model, cookie data, Google Advertising IDs, and Apple Advertising IDs. We may use your data to provide advertisements to you, to determine the relevance of advertisements, to measure the effectiveness of advertisements, to detect fraudulent advertisements or impressions, and to help make those advertisements more relevant to your preferences. When providing you with advertisements, we may transmit your personal data off of your device to third party advertisers so that they may serve relevant advertisements to you.

Use of Cookies

We may also collect data from you through the use of cookies and other technologies. This helps us understand how you use the AppGuard mobile application, serve you advertisements, and to understand any patterns that may be associated with your use of our services. This aids us in developing or improving our services in response to your needs or wants and in providing you with relevant offers from our advertisers.
We may use session or persistent cookies. Session cookies are only stored on your mobile device during your use of the mobile application and are automatically deleted when you close your mobile application. Persistent cookies are stored as a file on your mobile device that remain on your mobile device even after you close the AppGuard mobile application. Persistent cookies can be read by the mobile application that created the cookie when you use it again. We may use persistent cookies when we utilize Google Analytics or other analytics providers, which are intended to track the behavior of users within the AppGuard mobile application. We may also, from time to time, receive data from third parties including analytics providers or advertising networks such as Google, Facebook, or Apple

Disclosure of Personal Data

We only share or sell your personal data in limited circumstances. We may share, sell, or disclose your personal data with your consent or at your direction. We may also share or sell

your data with certain third parties to aid us in operating the AppGuard mobile application. For example, we may share your personal data with third parties, such as analytics providers, to utilize their software tools and measure the effectiveness of our advertisements. We may also share or sell your personal data, such as device IDs, with third party advertisers to help them determine whether they should serve an ad to you. The data that we share with or sell to these third parties does not include your email address, name, phone number, or username, but it may include your geographical location. We may also share your personal data with our accountants, auditors, insurers, or attorneys where doing so is necessary to protect the interests of AppGuard or to comply with any law or regulation. We may also share your personal data with government or law enforcement agencies when we are required to report our data processing activities, upon receipt of an exigent circumstances request, upon receipt of a duly authorized subpoena or court order, or where doing so is necessary to protect our users, our employees, our contractors, third parties, or property. Finally, we may share your personal data to a third party if we sell, transfer, or merge any part of our business or assets. In the event that we share your personal data in the sale, transfer, or merger of any part of our business or assets, this Privacy Policy will continue to apply to your personal data when transferred to the new entity.
To stop our collection and use of your personal data, you need only to delete your account by deleting the AppGuard mobile application.

Management, Protection, and Retention of Your Personal Data

To stop our collection and use of your technical data, you need only cease using and uninstall the AppGuard mobile application.
AppGuard is located in the European Union. We may transfer your personal data to countries outside of the European Union and outside the Brazilian territory, which may not offer the same level of protection. Many of our third-party service providers are located within the United States and their processing of personal data will involve an international transfer to several countries. We do our best to ensure a similar degree of security by transferring your personal data outside the Brazilian territory, complying with the requirements of the Law nº 13.709/2018 -Brazilian Data Protection Law (“Lei Geral de Proteção de Dados Pessoais” or “LGPD”).
We also put data security measures into place to protect your personal data. We allow access to your personal data only by employees and service providers who have a need to know or access your personal data on our instructions.
We will notify you and any regulatory body of any breach of your personal data or our security measures if and when we are legally required to do so.

Data Retention

We will only retain your personal data for so long as necessary to fulfill the purposes for which it is collected under this Privacy Policy or for the purposes of satisfying any legal, accounting, or reporting requirements. With respect to location data, technical data, usage and interaction data, and marketing data, we may retain this data for so long as it is relevant to the uses disclosed in this Privacy Policy. We may retain account data and public data for so long as you maintain an account with AppGuard , and we may retain this data for longer periods where there is a need to retain this data to comply with AppGuard legal obligations, such as the preservation of electronic evidence or compliance with a preservation order.

AppGuard does not, however, retain your sensitive personal information for longer than necessary for the uses disclosed herein, and your sensitive personal information will be used solely for the purposes of providing the functionality described above and required by our services and then it will be deleted.

Subject's Rights

Article 18 of the LGPD provides the following rights:
You do not need to pay a fee to exercise your rights. We will apply our best efforts to briefly respond you in accordance with the deadlines established by LGPD. To confirm your request, we may need to request specific information from you as a security measure to ensure that personal data is not disclosed to an unauthorized third party.

Third Party Links

Our services may include links to third party websites and applications. By clicking on third party links, you may allow third parties to collect or share data about you. We do not control these third-party links and you are advised their respective privacy policies.

Responding to Do Not Track Signals

You can generally opt-out of receiving personalized ads from third party advertisers and ad networks who are members of the Network Advertising Initiative (NAI) or who follow the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising by visiting the opt-out pages on the NAI website and DAA website. Our websites and mobile applicaations are not currently set up to respond to browser do-not-track signals, but you can configure your browser settings to reject all cookies or prompt you before a cookie is set.

Nevada Residents

If you are a resident of Nevada, you may provide notice to us to limit the sale of your PII to third parties for resale or licensing purposes. However, we do not sell your PII for such use. To notify us that you wish to limit the sale of your PII to third parties for resale or licensing purposes, you may send us an email to support@AppGuard.co with the subject line, "Nevada Do Not Sell Request," along with your name, address, and account information.

Virginia Residents

We do not control or process the personal data of at least 100,000 Virginia residents or control or process the personal data of at least 25,000 Virginia residents and derive more than 50% of our gross revenue from the sale of personal data. For these reasons, the Virginia Consumer Data Protection Act (VCDPA) does not apply to our collection and use of PII.

California Privacy Rights

The following rules apply solely to visitors and users of the AppGuard mobile application and website who are residents of the State of California. California residents have the right to be

notified which categories of PII are being collected and the purposes for which the PII is being used. In particular, AppGuard collected the following categories of PII (A, B, D, F, and G) as defined in the California Consumer Privacy Act within the last twelve months. AppGuard uses of this PII are detailed above in this Privacy Policy:

Category	Examples	Collected
A. Identifiers	Real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.	YES
B. Personal information categories listed in the California Consumer Records statute (Cal. Civ. Code § 1798.80(e))	Name, signature, address, telephone number, bank account number, credit card number, debit card number, or any other financial information.	YES
C. Commercial	Records of products purchased.	YES
D. Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
E. Geolocation data	Physical location or movements.	YES

AppGuard obtains these categories of PII directly from California residents when they use our mobile application, create an account with our mobile application, use features of our mobile application, or provide it to us as a part of a transaction or inquiry concerning our services. AppGuard also obtains these categories of PII indirectly from California residents while observing their actions on our website and from third parties or service providers that they have authorized to receive and share PII.

California residents have a right to request that we disclose what PII we collect from you and whether, and how, we disclose or sell that PII. California residents may also request that we delete any personal information collected or maintained by us from you.

California residents may also have the right to opt out of the sale of their personal information by contacting us or, where available, by clicking a link or icon associated with an advertisement. Specifically, this link or icon may state “Do Not Sell My Personal Information” or “Do Not Sell My Info.” By selecting this link or icon, you “Opt Out,” which means that you have opted out of the sale of your personal information as set forth in the California Consumer Privacy Act. However, even though you may have opted out, you may still see interest-based advertisements. To learn more about interest-based advertising across websites and additional opt-out choices, you can visit http://optout.aboutads.info. If you opt-out of the sale of your personal information but do not opt out of interest-based advertising more generally, you may still receive ads tailored to your interests based on PII that was not sold by us, personal information that was sold to downstream participants at least 90 days before you opted out, or personal information that was sold by other sources from which you have not opted out.

To submit a request for a list of the categories of PII collected from you or to request that AppGuard delete your PII, please email us at support@AppGuard.co.

To verify your request, we may request certain information from you to confirm that you are an AppGuard user, such as your phone number, username, email address, city, state, or geographic location. You may also designate an authorized agent to make a request to AppGuard to disclose or delete your personal information. To do so, you must provide AppGuard with proof that the individual or business has been appointed as your agent, such by providing a signed power of attorney form, and provide accurate responses to any

information requested by AppGuard that may be necessary to confirm that you are a AppGuard user, such as your phone number, username, email address, city, state, or geographic location. California residents have a right not to receive discriminatory treatment by AppGuard for their exercise of these rights conferred under California law.

Notification of Changes in the Privacy Policy

Subject to the application of your rights under the applicable legal provisions, we reserve the right to modify this Privacy Policy without notice in order to reflect technological developments, legislative and regulatory changes and good business practices. In the event that we change our Privacy Policy, an updated version of this Policy will reflect those changes and we will notify you of those changes by changing the effective date at the top of this Policy and other places that we deem appropriate.

Children Prohibited

Our services are not directed to, or open to, children under the age of 13. In using our services, you warrant that you are over the age of thirteen (13). If you are younger than 13, please do not use the AppGuard website or mobile applications and please do not provide personal data to us.

Global Operations

You understand and agree that we may store and process your data on computers located outside of the Brazilian territory, including, but not limited to, in the United States, European Union. By using the the AppGuard website and mobile applications, you agree to the collection and processing of your data outside of the Brazilian territory.

Contact Information

If you have any questions or suggestions regarding our Privacy Policy, or if your personal information is not accurate or complete, please contact our Data Protection Officer at: AppGuard support@AppGuard.co