

Privacy Policy – Phone Guardian

Available at: phoneguardianapp.com/pp/en.php

Privacy Policy

[See previous versions](#)

data.ai Privacy Policy for Mobile Applications (Phone Guardian)

Last Updated February 23, 2023

Our Privacy Policy Has Recently Changed.

The privacy and security of your information is important to us. We have made changes to our Privacy Policy that apply with respect to information that you provide on or after the date indicated in the "Last Updated" legend above. These changes include:

1. Additional detail regarding what personal information and other information we collect from you, and how we collect and use it;
2. Further descriptions of the parties with whom and for what purposes your information is shared; and
3. What rights you have regarding your personal information.

To learn more, please review the full data.ai Privacy Policy for Mobile Applications below.

data.ai cares about the privacy of individuals who use our mobile application, Phone Guardian (" **App**"). You can also learn more about the App at our website phoneguardianapp.com.

As used herein, " **data.ai**" or " **us/we/our**", refers to data.ai inc., a US company, acting by itself and/or through entities that are legally part of the data.ai family of companies (the " **Related Companies**"). Those Related Companies include, but are not limited to, data.ai Europe Limited, Mobidia Technology Inc., and Distimo BV See a list of Related Companies here: phoneguardianapp.com/related-companies.php. For more information about how data.ai processes your personal information when you visit our website at data.ai, please review <https://www.data.ai/en/legal/privacy/>.

Summary

This data.ai Privacy Policy for Mobile Applications (" **Policy**") explains how the App collects information about you and about how you use your mobile device, including information about the apps you use and websites you visit. data.ai processes and safeguards information we obtain from and about you when you use the App. The Policy also explains your rights and choices with respect to your personal information, and how you can contact us if you have any questions or concerns. No part of the App is directed to children under the age of 16, nor do we knowingly collect information from anyone under the age of 16 (see Section 7 of this Policy).

This Policy does not apply to other websites, mobile applications and services provided by data.ai. Please visit the privacy policy for the respective website, mobile application or service.

Your use of the App is subject to this Policy and the [Terms of Service](#) accessible on the App. **If any term of this Policy is unacceptable to you, please do not use the App and do not provide your personal information.**

TABLE OF CONTENTS

1. [HOW DATA.AI COLLECTS YOUR INFORMATION](#)
2. [HOW WE USE YOUR INFORMATION](#)
3. [HOW WE DISCLOSE YOUR INFORMATION](#)
4. [TRANSFERS TO OTHER COUNTRIES](#)
5. [DATA RETENTION](#)
6. [OUR COMMITMENT TO SECURITY](#)
7. [CHILDREN'S PRIVACY](#)
8. [DO NOT TRACK](#)
9. [YOUR RIGHTS AND CHOICES](#)
10. [THIRD-PARTY PLATFORMS](#)
11. [UPDATES TO THIS PRIVACY POLICY](#)
12. [HOW TO CONTACT US](#)

1. How data.ai Collects Your Information

For the purpose of this Policy, "**Personal Information**" means any information relating to an identified or identifiable individual or, when applicable, legal entity. An identifiable individual or legal entity is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier. We obtain Personal Information relating to you from various sources described below.

Where applicable, we indicate whether and why the provision of your Personal Information is a statutory or contractual requirement, as well as the possible consequences of failing to do so.

i. Personal Information Provided Directly by You When You Engage with Us

If you contact us directly, such as to request information, access the App, or connect with Customer Support, we may receive additional Personal Information about you, such as your name, email address, the content, date and time of your message, and our reply. We also may receive Personal Information if you complete a survey, such as demographic information (e.g., age, gender) and any other Personal Information you choose to provide.

ii. Personal Information We Collect About You When You Use the App

Depending on the mobile device operating system you use (i.e., iOS or Android) and the choices you make when you open the App for the first time or at any later stage in the App's Data Privacy Preferences, we collect the following Personal Information:

- Device-specific information: This includes your mobile device model, operating system, version number, web browser used, language and regional

- setting, carrier or network, time stamp and zone, device motion parameters;
- Information about your use of other apps and websites: This includes the frequency and length of time you spend on other apps and websites you visit as well as the dates and times of your interactions;
- Your approximate ("coarse") location: This includes latitude and longitude of the center of the nearest city without revealing your precise location or GPS data;
- Unique identifiers: This includes unique installation IDs, IP addresses, User Agents, Android IDs (on Android only) and other user and device identifiers;
- Crash-related information: This includes information about errors and crashes when accessing and using the App (e.g., lost connection to the Internet), such as date and time of crashes and crash traces;
- App usage analytics: This includes statistics about your interaction within the App, such as the number of daily active App users, how often and when users launch or close the App, which App screens users open and how they interact with different App features;
- Ad attribution and related user analytics: This includes information related to our marketing campaigns and user behavior, such as clicks on our ads, the webpage or application from which such ads were displayed, other user events and actions related to our marketing campaigns.

This App integrates several software development kits (" **SDKs**") that contain a set of tools from third-party providers that allow us to develop certain functionalities of this App. Please refer to Section 10 of this Policy for more details about the SDKs and the specific categories of Personal Information that these SDKs process, if you have consented to their use in the App's Data Privacy Preferences.

2. How We Use Your Information

i. When You Use This App

Use of a Virtual Private Network (" **VPN**") and Usage Access permission

This App uses a VPN (for iOS and Android devices) to collect information about your network connection. This information is used to detect any unencrypted network traffic and encrypt it by routing traffic through a secure server. We also use the Usage Access permission (for Android devices only) to collect information about how you use apps on your mobile device. This information is used to show which apps have made internet connections and have been encrypted by the VPN. Individual user information collected through the VPN or Android Usage Access permission is not shared with third parties, including our service providers.

Personal Information contained in the network traffic transmitted through the VPN and encrypted by us is processed as part of our service that we provide through this App.

Customer Service

To provide you with customer service when you contact us. Please note that if you seek help through the Help and Feedback section within the App, we use a third party to facilitate customer support on our behalf, and the Phone Guardian website privacy policy applies: phoneguardianapp.com/pp.php.

ii. When You Consent to the Processing of Your Personal Information

With your consent, data.ai will process your Personal Information for the purposes listed below. Your consent is voluntary and not a condition for using this App. You can withdraw your consent anytime in the Data Privacy Preferences in the App settings. Withdrawing your consent will not impact the legality of us having processed your Personal Information prior to you withdrawing your consent.

Market Research on Other Apps Usage

With your consent, part of the information we collect (as outlined below) through the VPN (iOS and Android) or Usage Access permission (Android) is used to conduct market research on mobile behavior. To understand how other apps are used and how popular they are, we collect and process information about your use of other apps—specifically, the frequency and length of time you spend on other apps, the websites you visit, and (Android only) when other apps are active—as well as your device-specific information (e.g., model, operating system and version number). Your approximate location (latitude and longitude of the center of the nearest city) helps us analyze such usage information on a geographical basis. We do not collect your precise location or GPS data.

Our market research typically aims at answering questions like the following:

- Which apps and websites are generally used in your country?
- How many people generally use a specific app or website?
- How much time is generally spent on social networks (e.g., Facebook, Twitter)?
- How many times per day is a specific app being used on a general basis?

Your consent also will allow us to store and gain access to unique, randomly-generated per-installation identifiers on your mobile device.

App Crash Reporting

To identify and fix performance issues with this App, we process information about your mobile device (e.g., model, coarse location) as well as other performance data. You also consent to Google LLC storing and accessing this information on your device, including a unique per-installation identifier that is only used in relation to crash reporting.

We use a third-party service to detect App crashes—Google LLC's Firebase Crashlytics in the U.S. (see Section 10 of this Policy)—to process:

- Device-specific information (e.g., model, operating system and version number);
- Per-installation identifier (a random installation identifier unique to Firebase);
- Coarse geographic location information inferred from your IP address (e.g., city, country); and
- Other crash-related information (e.g., date and time of crash and crash traces).

Firebase Crashlytics helps us to combine this information across different devices and operating systems to identify and fix problems with the App and to improve its performance. We do not combine Personal Information collected through Firebase Crashlytics with any other Personal Information we may have received from you for other purposes.

Your consent will allow us to disclose and process your Personal Information through Firebase Crashlytics. Your consent also will allow Firebase Crashlytics to store and gain access to a per-installation identifier on your mobile device.

Analytics & Remote Configuration

To improve the user experience of the App and notify users about upcoming App changes, we process information about your mobile device (e.g., model, coarse location) and your interaction within our App.

You also consent to Leanplum Inc. and Google LLC storing and accessing information on your device, including unique per-installation identifiers that are only used in relation to analytics and remote configuration.

To analyze how users generally interact with our App, identify problems we should fix, and determine which features we should support or remove, we use third-party tools—Leanplum Inc.'s services and certain of Google LLC's Firebase services in the U.S. (see Section 10 of this Policy)—to process:

- Per-installation identifiers (a random installation identifier unique to Firebase and a separate random installation identifier unique to Leanplum);
- Device-specific information (e.g., model, operating system and version number);
- User interaction statistics, such as the number of daily active users, how often and when users launch or close our app, which App screens users open and how they interact with different App features; and
- Coarse geographic location information inferred from your IP address (e.g., city, country).

For example, we use these services to conduct A/B testing. These services also allow us to notify users about upcoming app changes (e.g., to send in-app messages or show push notifications). We do not combine personal information collected through Firebase or Leanplum with any other personal information we may have received from you for other purposes.

Your consent will allow us to disclose and process your Personal Information through the Leanplum and Firebase services we currently use. Your consent also will allow Leanplum and Firebase to store and gain access to per-installation identifiers on your mobile device.

Ad Attribution and Related User Analytics

To determine the effectiveness of our own marketing campaigns, we process information about your mobile device, coarse location data, and how you interact with our marketing campaigns. You also consent to AppsFlyer Ltd. storing and accessing this information on your device, including a unique per-installation identifier that is only used in relation to ad attribution and related user analytics.

To determine the effectiveness of our own marketing campaigns and which marketing channels work best for us, we use a third-party tool—AppsFlyer Ltd.'s Measurement Suite and Marketing Analytics (" **AppsFlyer**") in Israel (see Section 10 of this Policy)—to process:

- Device-specific information (e.g., model, operating system and version number);
- Per-installation identifier (a random installation identifier unique to AppsFlyer);
- Coarse geographic location information inferred from your IP address (e.g., city, country); and
- Other information related to our marketing campaigns and user behavior (e.g., clicks on our ads, the webpage or application from which such ads were displayed, other user events and actions related to our marketing campaigns).

For example, AppsFlyer helps us understand when a user has finished setting up this App and if a user remains active on this App after a certain number of days. We do not combine personal information collected through AppsFlyer with any other personal information we may have received from you for other purposes.

Your consent will allow us to disclose and process your Personal Information through AppsFlyer. Your consent will also allow AppsFlyer to store and gain access to a per-installation identifier on your mobile device.

iii. Processing of your Personal Information for Other Purposes

data.ai also processes your Personal Information in compliance with legal obligations and/ or our own legitimate interests as a company, including to:

- Protect and enforce data.ai's legal rights, including our IP rights and other assets;
- Meet legal compliance obligations, including corporate reporting, legal and regulatory compliance and fiduciary obligations;
- Protect the security of our products, services, and systems, manage business continuity and disaster recovery operations;
- Enable access to and use of the App, App updates and other processing necessary for enforcement of our Terms of Service and in general the operation of the App.

iv. Overview of Processing Activities and Legal Bases for EU users

Purpose	Consent	Contract	Legal Obligation	Legitimate Interest
Use of a VPN		•		
Use of Usage Access permission (Android)	•	•		
Contacting us via methods described in Section 12 of this Policy		•		•
Market Research on Other Apps Usage	•			
App Crash Reporting	•			
Analytics & Remote Configuration	•			
Ad Attribution and Related User Analytics	•			
Enable access to and use of the App, manage App updates, and other processing necessary for enforcement		•		

Purpose	Consent	Contract	Legal Obligation	Legitimate Interest
of our Terms of Service and in general the operation of the App				
Protect the security of our products, services, and systems, manage business continuity and disaster recovery operations		•	•	
Protect and enforce data.ai's legal rights, including our IP rights and other assets				•
Meet legal compliance obligations, including corporate reporting, legal and regulatory compliance and fiduciary obligations			•	
Participate in surveys	•			•

3. How We Disclose Your Information

Corporate Affiliates

data.ai may share Personal Information with our Related Companies in the ordinary course of business and for the purposes of providing the services set forth in this Policy. See a list of our Related Companies here: phoneguardianapp.com/related-companies.php.

Service Providers

Depending on the choices you make in the App's Data Privacy Preferences, we share your Personal Information with third-party service providers (see Section 10 of this Policy). We also share your Personal Information with our data analytics service providers and customer-service support. We enter into confidentiality and data processing agreements with these providers to provide appropriate and suitable safeguards for their processing of your Personal Information. See a list of our service providers here: phoneguardianapp.com/related-companies.php.

As Required by Law and Similar Disclosures

Subject to applicable local laws and regulations we disclose Personal Information we have about you: (i) if we are required to do so by law, regulation, or legal process, such as a court order or subpoena; (ii) in response to requests by government agencies, such as law enforcement authorities; (iii) when we believe disclosure is necessary or appropriate to protect against or respond to physical, financial or other harm, injury, or loss to property; or (iv) in connection with an investigation of suspected or actual unlawful activity.

Merger, Sale, or Other Asset Transfers

Subject to possible restrictions under applicable local laws and regulations, data.ai may disclose your Personal Information to a potential or actual acquirer, successor, or assignee as part of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in bankruptcy or similar proceedings).

Aggregated Information

If you have consented to market research on other apps usage, we will aggregate your Personal Information with other information. We only share such information in an anonymized and aggregated manner with our Related Companies and for the purpose of providing data.ai services to third parties or publicly. We do not sell your Personal Information.

4. Transfers to Other Countries

The App is provided from the United States and other locations, and we may transfer your Personal Information to multiple countries throughout the world, including the United States, in accordance with applicable local laws and regulations. These countries may not have the same high level of protection as the data protection laws in the country from which you initially provided the information.

Where required to comply with applicable law, we rely on appropriate and suitable safeguards including EU Standard Contractual Clauses to transfer Personal Information to countries outside the European Economic Area ("EEA") or Switzerland as well as the Addendum B.1.0 issued by the Information Commissioner of the UK (as it is revised from time to time) for transfers of Personal Information outside the United Kingdom, where an adequate level of protection is not already guaranteed. We also transfer Personal Information to countries for which an adequacy decision of the EU Commission or other regulatory agency exists.

See a list of our Related Companies and service providers, their locations as well as the transfer safeguards applied or whether an adequacy decision exists here: phoneguardianapp.com/related-companies.php.

You may contact us as specified in "How to Contact Us" (see Section 12 of this Policy) to obtain a copy of the appropriate and suitable safeguards we use to transfer Personal Information outside of these countries.

5. Data Retention

Personal Information will be stored and kept as long as needed to carry out the purposes described in this Policy or as otherwise required by applicable law. Unless we are required or permitted by law to keep this information for a longer period of time, when this information is no longer necessary to carry out the purposes for which we process it, we will delete your Personal Information or keep it in a form that does not permit identifying you. When determining the retention period, we take into account various criteria, such as the type of services requested by or provided to you, the nature and length of our relationship with you, possible re-enrollment to use our App, the impact on the App functionality we provide if we delete some Personal Information from or about you, mandatory

retention periods provided by law and the statute of limitations, and our use of your information for aggregated market research. For example, we delete your IP address within 30 days of collection and we delete your unique installation identifier within 3 years of collection.

6. Our Commitment to Security

data.ai cares about the security of your information, and employs physical, technological and administrative measures to protect the information you submit via the App against loss, theft, and unauthorized access, use, disclosure or modification. For more information on the security measures taken by us, please contact us at the e-mail address provided in "How to Contact Us" (see Section 12 of this Policy). However, we cannot ensure or warrant the security of any information you transmit to us or guarantee that information on the App may not be accessed, disclosed, altered or destroyed. Electronic communications sent to or from the App may not be secure. You should use caution whenever submitting information online and take special care in deciding what information you send to us. If you have reason to believe that your Personal Information is no longer secure, please notify us at the e-mail address provided in "How to Contact Us" (see Section 12 of this Policy).

7. Children's Privacy

We do not knowingly collect, maintain, or use Personal Information from children, and no part of the App is directed to children. If you learn that your child has provided us with Personal Information without your consent, then you may alert us at PG-privacy@data.ai. If we learn that we have collected any Personal Information from children under 16, then we will promptly take steps to delete such information. References to "child" and "children" in this Policy refer to a person or persons under the age of 16 (or such greater age required in the applicable jurisdiction for an App user to be bound by a contract without guardian consent).

8. Do Not Track

Some web browsers incorporate a "Do Not Track" feature. Because there is not yet an accepted standard for how to respond to Do Not Track signals, our App does not currently respond to such signals. If you want to restrict ads in general on your devices you may opt out from ad tracking by enabling "Limit Ad Tracking" or "Opt Out of Ads Personalization" (as applicable to your device) in your device settings.

9. Your Rights and Choices

i. Global Rights & Choices

We provide you with certain choices with respect to your Personal Information and where applicable, marketing activities, with respect to our App:

- Advertising ID. You can reset the advertising identifier randomly assigned to your device at any time and can opt out of personalized ads by denying such permissions on your device. When you deny these permissions, advertisers and their measurement solutions will receive a blank device ID in place of a device-specific ID.

In addition, subject to applicable laws and any legal obligations, we provide all users with certain rights in connection with our processing of Personal Information through the App:

- Right to Object. You have the right to object at any time to the processing of Personal Information on grounds relating to your particular situation, including a right to object to the processing of your Personal Information for processing performed on the basis of legitimate interest, unless we are able to demonstrate overriding compelling legitimate grounds. If you'd like to exercise your right to object, you can do so by going to the Data Privacy Preferences page in App settings and turning all the toggles off.
- Right to Know/Access. You have the right to obtain confirmation from us as to whether we are processing your Personal Information and the right to access and receive a copy of such Personal Information. You can access this information by going to the Data Privacy Preferences page and selecting "Data Export."
- Right to Delete/Erasure. If you have consented to sharing any of your Personal Information with us and you want to erase it, please delete the App from your phone. Once you delete the App from your device, we will no longer receive any of your information, including Personal Information, and we will no longer be able to identify you as a user of the App because your information will be anonymized. If you would like to request any information about the erasure of Personal Information, please submit a request at PG-privacy@data.ai.
- Right to Rectify/Correct Inaccurate Information. If we process inaccurate, incomplete, or outdated Personal Information, you have the right to update or correct your Personal Information which you submit for support cases (e.g., your email address). However, we do not have an ability to rectify/correct any of your other Personal Information collected through your use of the App, as we can only delete it. If you'd like to delete your Personal Information, please follow the directions as described in the "Right to Delete/Erasure" subsection above. Once you have deleted the App, any Personal Information that you had provided through the App is anonymized.
- Right to Withdraw Consent. Once you have consented to the collection of your Personal Information through the App, you may withdraw your consent at any time by going to the Data Privacy Preferences page in App settings. Please note that your withdrawal of consent would not affect the lawfulness of processing based on consent before it was withdrawn.
- Right to Data Portability. You have the right to receive the Personal Information concerning you in a structured, commonly used and machine-readable format and the right to transmit that information data to another company where feasible. You can exercise this right by going to the Data Privacy Preferences page and selecting "Data Export."
- Right to Restrict. You have the right to restrict us from continuing to process your Personal Information under certain circumstances (e.g., you contest the accuracy of your Personal Information or when you believe that we are processing your Personal Information beyond the original purpose). To exercise this right, please go to the Data Privacy Preferences page in App settings and turn the toggles off. If you'd like to delete all your Personal Information, you can do so by following the directions above in the "Right to Delete/Erasure" subsection above.
- Right to Lodge a Complaint. Depending on your country of residence, you have the right to lodge a complaint with the competent data protection supervisory authority. You can, for example, contact the supervisory authority in the EU Member State of your residence, place of work or place of the alleged infringement. For more information on how to lodge a complaint in the EU/EEA, please see https://edpb.europa.eu/about-edpb/board/members_en.
- Right to Opt Out of the Sale of Personal Information. We do not sell or share your personal information as defined under California and other state laws and we do not collect any sensitive personal information for the purpose of inferring characteristics about you.
- Right to Appeal. Certain states in the United States (e.g., Colorado, Connecticut, and Virginia) allow you to appeal instances of where we are not able to honor your exercise of your Personal Information rights. If you are in one of these states and wish to appeal a decision we made with respect to exercising a right about your Personal Information, you must email us at PG-privacy@data.ai and in the email subject line include (a) your state of residence and (b) the words "Appealing Rights Decision," and (c) in the email body provide an explanation of the basis of your appeal.
- Right to Non-Discrimination. We will not discriminate against you for exercising any of your privacy rights, including those under California law.

data.ai does not process an opt-out preference signal (e.g., the Global Privacy Control) in connection with your use of the App because we do not sell or share your personal information.

If you wish to exercise your rights or have any questions about exercising your rights, please contact us using the information listed in "How to Contact Us" (see Section 12 of this Policy).

ii. Additional Information for California Residents

Verification and Authorized Agent

To exercise your rights, please follow the instructions above and the contact information in the "How to Contact Us" section (see Section 12 of this Policy). We will confirm receipt of your requests and respond within 30 calendar days, unless additional time is needed, in which case we will provide notice and an explanation of the reason. Also, to respond to your request to correct, request to know, or request to delete, we must verify your identity or authority to make the request and confirm the Personal Information relates to you or to others. To do so, we collect your email address to verify your identity through the App. We also may contact you by email (if you have provided it to us) to verify your identity and ask you additional questions so that we can match your identity with the data we have about you. In some instances, we may ask you to declare under penalty of perjury that you are the consumer whose Personal Information is the subject of the request. If we cannot verify your identity, we may reject your request in whole or in part.

You also may designate an authorized agent to make a request for you. To use an authorized agent, we may require: (1) your signed permission designating the authorized agent; (2) evidence that the authorized agent has power of attorney under the California Probate Code; or (3) proof that the authorized agent is registered with the California Secretary of State and that you have authorized such authorized agent to be able to act on your behalf. We may deny a request from an authorized agent who does not submit sufficient proof.

Collection of Personal Information, its Purpose, and Disclosure

In the preceding twelve (12) months, we have collected categories of Personal Information as explained in Section 1 of this Policy ("How data.ai Collects Your Information").

Purposes

In the preceding twelve (12) months, we have used and disclosed the aforementioned categories of Personal Information from the sources described in Section 2 ("How We Use Your Information") and Section 3 ("How We Disclose Your Information") of this Policy for business and commercial purposes, including:

- Debugging to identify and repair errors in the App that impair existing intended functionality and improve its performance;
- Providing services (including providing customer service, in-app messaging about App features, optimizing and figuring out the features that users are using in the App, figuring out the effectiveness of our marketing of the App); and
- Undertaking internal research for technological development and demonstration (i.e., to develop new products or features) and to maintain, improve, upgrade, and enhance the App.

We also have used and disclosed the Personal Information we collect for commercial purposes to provide you with our App, as described in Sections 2 and 3 of this Policy.

In the preceding twelve (12) months, we have disclosed your Personal Information for a business or commercial purpose to the following categories of third parties:

Categories of Personal Information	Categories of Third Parties
Device-Specific Identifiers, such as your mobile device model, operating system, version number, web browser used, language and regional setting, carrier or network, time stamp and zone, device motion parameters	Our Related Companies App crash reporting service provider(s) Analytics & remote configuration service provider(s) Ad attribution and related user analytics service provider(s)
Geolocation data	Our Related Companies App crash reporting service provider(s) Analytics & remote configuration service provider(s) Ad attribution and related user analytics service provider(s)

10. Third-Party Platforms

Our App relies on SDKs and related services provided by third parties listed below. Depending on the choices you make in the App's Data Privacy Preferences, these SDKs will be activated or deactivated:

- **Firebase SDK** , provided by Google LLC—Services used on Android: Crashlytics, Cloud Messaging, Remote Config, Analytics for Firebase, App Distribution; Services used on iOS: Crashlytics, Analytics for Firebase

You can find more information on Privacy and Security in Firebase, including on the Personal Information processed by Firebase and the device information collected by Crashlytics, at <https://firebase.google.com/support/privacy>.

- **AppsFlyer SDK** , provided by AppsFlyer Ltd.—Services used: Measurement Suite and Marketing Analytics

You can find AppsFlyer's Services Privacy Policy, including information on the Personal Information processed by AppsFlyer, at <https://www.appsflyer.com/legal/services-privacy-policy/>.

- **Leanplum SDK** , provided by Leanplum Inc.

You can find more information on the Personal Information processed by Leanplum at <https://docs.leanplum.com/reference/user-and-device-tracking>.

[None of the information collected through VPN or Android Usage Access permission is ever shared with the third-parties listed above.]

11. Updates to this Privacy Policy

We reserve the right to change this Policy at any time. We will post any amendments to this Policy on this page, and the revised version will be effective the date it is posted, which is identified at the top of the page. If we materially change the ways in which we process your Personal Information previously collected from you, we will notify you through our App or any other means. We encourage you to review the Policy, which may be updated from time to time. Your continued use of our App after such amendments will be deemed your acknowledgement of these changes to this Policy.

12. How to Contact Us

If you have any questions or concerns about data.ai's privacy practices or about this Policy, or would like to exercise your rights in relation to your Personal Information, you may:

- Contact data.ai via e-mail at: PG-privacy@data.ai, or
- Write us at:

data.ai inc. Legal Department 44 Montgomery Street, Third Floor San Francisco, CA 94104 USA

data.ai's Data Protection Officer may be contacted via email (PG-privacy@data.ai) or at the following address:

data.ai inc. Legal Department ATTN: Data Protection Officer 44 Montgomery Street, Third Floor San Francisco, CA 94104 USA

Phone: +1-844-277-2664

data.ai inc. is the entity responsible (data controller) for the processing of your Personal Information.