Lookout, Inc.

Lookout for Work Application

Privacy Notice

Effective Date: 11/17/2020

Origination Date: 10/24/2016

Lookout for Work Application Privacy Notice

Lookout, Inc. (“Lookout,” “we,” or “us” or “our”) firmly believes that your privacy is as important as your security, so we want to be transparent about the data we collect to help safeguard your device and the security of your employer. Lookout provides you with this Enterprise Privacy Notice (the “Notice”) to describe our information practices with respect to our Lookout for Work application (the “Services”). This Notice governs the data collected from or about you through your installation and activation of our Services on your mobile device. By downloading and activating the Services, you acknowledge the data collection, use, disclosure, and storage practices described in this Notice. Any information that is collected from you by Lookout other than through the use of the Services will be subject to a different privacy notice.

You may have been directed to download and install the Services as a result of your employment by an organization that either (1) requires all or some of its workforce to install the Services or (2) requires all or some of its workforce to install a mobile device management suite that includes the Services. Please understand that, unless explicitly specified otherwise herein, this Notice governs only our information practices with respect to our Services. To the extent you have questions or requests regarding the data collection, use, disclosure, and security practices of your employer (“Employer”) or a mobile device management provider (“MDM Provider”), or about data that we collect on behalf of your Employer, you should direct those questions or requests to those parties.

Lookout reserves the right to change this Notice at any time to reflect changes in the law, our data collection and use practices, the features of the Services, or advances in technology. If we make material changes to this Notice, then we will endeavor to notify you. If you take exception to the information contained herein, then you should cease your use of the Services.

We have structured this Notice to answer some general questions about our Services. This Notice contains answers to the following:

1. What is the Lookout for Work application?

The Lookout for Work application is a mobile security solution that protects mobile devices and enterprises from threats and compliance violations with corporate policies. Leveraging a global sensor network of over 100M sensors, Lookout delivers predictive security by using machine intelligence to identify complex patterns that indicate risk patterns that would otherwise escape human analysts. When a threat has been detected, Lookout provides

employees and administrators remediation options (e.g., uninstall app, invoke conditional access).

2. What data does Lookout collect from your mobile device?

To protect your mobile device and your Employer from threats, Lookout collects certain categories of data from your device. This data **may** include:

- **Analytics Data**, used to analyze product performance on your device,
- **Application Data**, including metadata of all applications installed on your mobile device (including, but not limited to, the names of the apps and the versions of the apps), and in certain circumstances, we may also collect a copy of the application,
- **Configuration Data**, such as whether your device is configured to allow root access or whether hardware restrictions of the device have been removed,
- **Device Data**, including the device and MDM identifiers of your mobile device,
- **Firmware/OS Data,** including the manufacturer and model of your mobile device, certain technical settings of your mobile device (including the display size of your mobile device and firmware version), the type and version of operating system on your mobile device,
- **Identification Data,** such as your work email address is optionally collected unless your employer uses the Privacy Controls feature in our Services,
- **Network Data**, including metadata about networks your mobile device connects to (including, but not limited to, the SSID of the network, or the unique MAC/BSSID address of network equipment), and IP address (which can indicate your country and geolocation),
- **Web Content Data**, including URLs and domains for malicious content and content that needs additional analysis.

Please note that we need certain types of information so that we can provide the Services. If you do not provide us with such information, or if we are asked to delete it, you may no longer be able to access the Services.

3. Does Lookout read or review my emails or see my photos?

No. Lookout collects only metadata about applications on your device, or the application itself. Lookout does not collect user data you enter into those applications. Because Lookout does not collect any user data you enter into the applications on your mobile device, Lookout does not collect, read, review, or scan your emails, or text messages. Lookout does not collect your photos, or videos, but may scan such files locally on the device to protect you from certain threats that hide inside photo or video files.

4. Does Lookout collect any other data about me outside of my mobile device?

Your Employer may provide Lookout with your email address to enable the Services. If the Services are integrated with an MDM solution and Privacy Controls are turned on, Lookout will not collect your email address, though your email address may be accessible by Lookout through the MDM.

If you installed the Services as part of a MDM Provider's product, we may also collect or have access to information about you from that MDM Provider, which may include your email address. Please contact the applicable MDM Provider regarding that provider's privacy practices.

Lookout may also collect other information about you if you provide such information to us directly by contacting us and voluntarily disclosing such information.

5. When does Lookout collect data from my mobile device?

After you download, install, and activate the Services, Lookout will immediately begin collecting data from your device to ensure it is free of threats and in compliance with corporate policies. As you install or access applications on your mobile device, we will scan those applications for potential security threats.

6. How does Lookout use the data collected from my mobile device?

We use the data collected for various business and commercial purposes. For example, the data we collect from your mobile device enables us to detect threats to you and/or your Employer, to improve our Services, and to improve our other product offerings. We may also combine data collected from your mobile device with data collected from third parties to improve our Services. This data is pseudonymized. If results of our analysis is shared publicly it will be done so in aggregate and pseudonymized to protect your privacy and the privacy of your Employer. How we use your information will vary depending on the type of data as described below:

- **Application Data**. We use this data to provide our Services by conducting scans of application files to determine if any applications are behaving maliciously. In analyzing the applications on your mobile device, if we encounter an application we have not previously analyzed, we may download a copy of part or all of the application to analyze and determine if it poses a risk, depending on how your Employer has configured the Services. As stated in Section 3, we do not collect any user data you enter into the applications when downloading a copy of the application.
- **Configuration Data.** We analyze configuration data about your device to determine whether your device has been modified, compromised or been configured insecurely, such as being infected, rooted or jailbroken or not having a passcode set.
- **Device Data**. We use device or MDM identifiers to help match your device to a device in a third-party system, such as a Mobile Device Management solution, so that we can report to that system whether your device has encountered any threats.
- **Firmware/OS Data.** Lookout uses this information to identify compromised firmware and operating systems and let you know when there is a security update available for your device.
- **Identification Data.** We optionally collect your work email address to help provide contextual information when we notify your Employer about threats you encounter. We never email you without consent.
- **Network Data.** Attackers may use internet connections, including Wi-Fi, to steal data, which is known as a man-in-the-middle attack (MitM). We may use the SSID to help identify these MitM attacks. Lookout may also approximate your country and region using your IP address, but Lookout does not read, store, or transfer users' actual device location (GPS) data. We pseudonymize data and aggregate this information to produce popularity of applications by region, and to perform our mobile threat analysis. This information will remain pseudonymized to ensure data privacy.
- **Web Content Data**. Lookout uses a VPN interface to analyze traffic on your device for threats as part of our Safe Browsing feature to block access to malicious or phishing websites. The content and history of your traffic will not be shared with your Employer, and your Employer will only be notified if you encountered a threat.

In accordance with the General Data Protection Regulation, the legal basis for using your information as set out in this Notice will depend on your relationship with your Employer and on your Employer's use case and may include the following: (a) Use of your personal information is necessary to perform our obligations under any contract with you (for example, for your employer's performance of its employment contract, or for Lookout to comply with the Terms of Service which you accept by downloading and using our apps); or (b) Where use of your information is not necessary for performance of a contract, use of your information is necessary for our legitimate interests or the legitimate interests of the Employer or others (for example, to ensure the security of the Services, operate the Services, ensure safe environments for our and your Employer's personnel and others, make and receive payments, prevent fraud and to know the customer to whom we are providing the Services); and compliance with legal requirements, such as those requiring appropriate data security.

7. Does Lookout share my data with anyone else?

As an enterprise product, certain data is shared with your Employer, or anyone authorized by your Employer to view such data. Through the Services dashboard, Employers or their authorized persons are granted access to certain information related to the security of your mobile device. Your Employer may be able to see your device attributes such as device model and carrier. Your Employer may have visibility into applications that we have identified as malicious, as well as those that are in violations of any applicable company policy of your Employer. Please contact your Employer about how such violations of applicable company policies may affect you.

If you installed and activated our Services as part of a product by an MDM Provider, we may share the security and activation status of your mobile device with that MDM Provider.

We may share any data related to you with third parties, including other members of our corporate family, and service providers or partners that we have engaged to perform business-related functions on our behalf. This may include service providers that: (a) provide customer, technical, or operational support; (b) fulfill orders and user or Employer requests; (c) host our Services; (d) maintain databases; (e) analyze data for product improvement and enhancement purposes; and (f) otherwise support or market our Services or any other Lookout products. We may disclose any data related to you in response to any subpoenas, court orders, or other legal process we receive, or to establish or exercise our legal rights or to defend against legal claims. If we receive a request for information from a local, state, federal, or foreign law enforcement agency, we will endeavor to transmit those requests to your Employer for processing by the Employer, but we reserve the right to respond directly and provide the information requested where we deem such response legally appropriate. We may disclose any data related to you when we believe in good faith that such disclosure is appropriate in order to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of this Notice, License Agreement or the End User Agreement for the Services, and/or to protect the rights and property of Lookout, our employees, users and the public. This may involve the sharing of your information with law enforcement, government agencies, courts, and/or other organizations.

We may share any data related to you in connection with any merger, reorganization, a sale of some or all Lookout assets, or a financing or acquisition of all or a portion of our business by another company.

8. Does Lookout sell my personal information to anyone else?

No. Lookout does not sell the Personal Information (as we understand that term to be defined by the California Consumer Privacy Act) of its users. As mentioned above in Section 6, we may aggregate data collected from your mobile device with data collected from third parties to improve our Services, but this data is pseudonymized and does not contain any personal information.

9. What information can my Employer NOT see?

Lookout only shares information with your Employer that is necessary for them to ensure that your device is free of threats and compliant with corporate security policies. Lookout does not, for example, enable your Employer to see the contents of your email, browsing history, contacts, calendar, text messages, non-malicious apps you have installed (unless the use of such an app is in violation of any applicable company policy of your Employer), or track your location.

10. Do you use my data for marketing purposes?

We do not use data collected by automated means from your mobile device to sell products to you, nor do we share it with third parties for their marketing purposes. We may aggregate information collected from your device to conduct research and provide insight into mobile device security and threats. In these instances, the aggregated information included in the research is pseudonymized.

11. How does Lookout protect my data and for how long is it retained?

We have implemented reasonable administrative, technical and physical security measures to protect against the unauthorized access, destruction or alteration of your information. These safeguards are tailored to address the sensitivity of the information that we collect, process and store and as well as to the current state of technology.

Although we take appropriate measures to safeguard against unauthorized disclosures of information, because no method of transmission over the Internet or method of electronic storage is 100% secure, we cannot assure you that information that we collect will never be disclosed in a manner that is inconsistent with this Notice.

Our policy is to retain personal data only as long as reasonably necessary to provide our Services to you and others or as otherwise required for legal compliance purposes. We may delete your data after 60 days if your account is inactive and as otherwise provided in our Terms of Service. Information may persist in copies made for backup and business continuity purposes. In this situation all data is secured with 256-bit encryption at rest.

12. Where does Lookout store my data?

Lookout is a San Francisco-based company with servers housed in the United States. Personal Data collected from users outside the United States is transferred to the United States. If you are using the Services from outside the United States your information may be transferred to, stored, and processed in the United States where our servers are located and our databases are operated. We may also transfer your information to other countries where Lookout or our affiliates, subsidiaries and service providers operate facilities.

These countries may have data protection laws that are different to the laws of your country and which, in some cases, may not be as protective. However, wherever we transfer and process your information we take steps to ensure that your Personal Data remains protected in accordance with this Notice and applicable data protection laws. If you are a Resident of the European Economic Area ("EEA"), the United Kingdom or Switzerland we use a variety of legal mechanisms to help ensure your Personal Data and rights are protected, including standard contractual clauses approved by the European Commissions for the transfer of personal data to third countries.

Lookout has also self-certified with the E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data from E.U. States, the United Kingdom and Switzerland. These frameworks were developed to enable companies to comply with data protection requirements when transferring personal data from the European Union, the United Kingdom and Switzerland to the United States. To learn more about the Privacy Shield, and view our Privacy Shield certification, please visit http://www.privacyshield.gov.

As a Privacy Shield certified organization, Lookout adheres to the Privacy Shield Principles with respect to Personal Data transferred from the European Union, the United Kingdom and Switzerland to the United States. As required under the Principles, when Lookout receives information under the Privacy Shield and then transfers it to a third-party service provider acting as an agent on Lookout's behalf, Lookout has certain liability under the Privacy Shield if both (i) the agent processes the information in a manner inconsistent with the Privacy Shield and (ii) Lookout is responsible for the event giving rise to the damage.

If you have any questions or complaints about Lookout's privacy practices, including questions related to the Privacy Shield, you may contact us at the email address or mailing address set forth under "Contact Us if You Have Any Questions or Concerns." We will work with you to resolve your issue.

13. What are my data rights and choices?

If you are a Resident of the EEA, the United Kingdom or Switzerland, then in accordance with the General Data Protection Regulation ("GDPR"), you may have the following rights:

- **Access.** You have the right to request a copy of the Personal Data that we are processing about you. If you require additional copies, we may need to charge a reasonable fee;

- **Rectification.** You have the right to require the correction of any mistake in the Personal Data, whether incomplete or inaccurate, that we hold about you;
- **Deletion.** You have the right to require the erasure of Personal Data concerning you in certain situations, such as where we no longer need it or if you withdraw your consent (where applicable);
- **Portability.** You have the right to receive the Personal Data concerning you that you have provided to us, in a structured, commonly used, and machine-readable format and have the right to transmit that data to a third party in certain situations;
- **Objection.** You have the right to (i) object at any time to the processing of your Personal Data for direct marketing purposes and (ii) object to our processing of your Personal Data where the legal ground of such processing is necessary for legitimate interests pursued by us or by a third party.
- **Restriction.** You have the right to request that we restrict our processing of your Personal Data in certain circumstances, such as when you contest the accuracy of that Personal Data;
- **Withdrawal of consent.** If we rely on your consent (or explicit consent) as our legal basis for processing your Personal Data, you have the right to withdraw that consent at any time.

If you wish to exercise any of these rights, please contact your Employer. Where Lookout is acting as a data controller, you may also contact us using the contact information below to exercise these rights. In appropriate circumstances, we may route the request to the Employer and follow their instructions in addressing it. We will respond to your request in a timely manner and no later than within 30 days. In certain situations, however, Lookout may not be able to provide access to or delete all of the Personal Data that it holds about you.

Additionally, if you are a resident of the EEA, United Kingdom or Switzerland and are dissatisfied with the manner in which we have addressed your concerns about our privacy practices, you may seek further assistance, at no cost to you, from our designated Privacy Shield independent recourse mechanism, which you can learn more about by visiting https://www.jamsadr.com/eu-us-privacy-shield. You also have a right to lodge a complaint with the relevant supervisory authority. However, we encourage you to contact us first, and then we will do our very best to resolve your concern. Residents of the European Union may also select binding arbitration for unresolved complaints, but prior to initiating such arbitration, you must: (1) contact Lookout and afford us the opportunity to resolve the issue; (2) seek assistance from Lookout's designated independent recourse mechanism above; and (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue. To find out more about the Privacy Shield's binding arbitration scheme please see https://www.privacyshield.gov/article?id=ANNEX-I-introduction. Each party shall be responsible for its own attorney's fees. Please be advised that, pursuant to the Privacy Shield, the arbitrator(s) may only impose individual-specific, non-monetary, equitable relief necessary to remedy any violation of the Privacy Shield Principles with respect to the individual. Lookout is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

You may have certain rights under applicable law, including the General Data Protection Regulation and the California Consumer Privacy Act. If you wish to exercise any of those rights, please contact your Employer. You may also contact us using the contact information below.

14. How can I contact you with more questions?

If you have additional questions, we encourage you to contact your Employer. You may also direct questions to our Data Protection Officer at privacy@lookout.com or by postal mail at Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA 02108. Residents of the EEA contact us by mail at Lookout, Inc., Attn: G.J. Schenk, SVP International Sales, Florapark 3, 2012 HK Haarlem, Netherlands.