# Lookout Personal Privacy Policy

Origination Date: 15/11/2016
Revision Date: 22/05/2018
Status: Approved

## Revision History

Lookout, Inc. controls this document and therefore any printing of the material will constitute a "reference" copy. Users are responsible for confirming they have the current revision. When any part of this information requires an update, the entire document shall be reissued.

| Release | Date | Description | Submitted By |
|---|---|---|---|
| 1.0 | 22/09/2016 | Initial draft | Marcelo Guerra |
| 2.0 | 26/09/2017 | Updated | Joseph Leung |
| 3.0 | 01/04/2018 | Updated to capture product changes and describe regulatory updates. Moved Document History details to end of document. | Kimberly Snow |
| | | | |

## Effective Date: 25 May 2018

This document is our Privacy Policy, which describes what information we collect from you and how we use it. It is important that you read the Privacy Policy along with the Lookout Terms of Service (available at www.lookout.com/uk/legal/consumer-terms) because both apply to your use of the Lookout Personal App. Our Privacy Policy applies to our websites and mobile websites including at www.lookout.com, our Lookout Personal App, and all other Lookout services provided as part of the Lookout Personal App (as that term is defined in our Terms of Service).

The Lookout Enterprise Mobile Endpoint Security product privacy policy is described in the Lookout Enterprise Privacy Statement.

This Privacy Policy describes the collection and use of Personal Data (PD). Personal Data (PD) collected from you includes data elements such as your name, email address, phone number and/or your mobile device's unique identifier, among other things. The term Personal Data also encompasses personally identifiable information and personal data as defined in the GDPR General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR").

Lookout reserves the right to change this Privacy Policy to reflect changes in the law, our data collection and use practices, the features of our services, or advances in technology. Please check this document or web pages provided on Lookout.com periodically for changes. By continuing to use our services, you accept those changes and agree to be bound by the updated policy. Please contact us at privacy@lookout.com if you have any questions about this Privacy Policy. This policy can be accessed from the Lookout mobile application login screen, from the settings in the Lookout Personal App, and from our company's website.

## Products Offered in the Lookout Personal App

Lookout offers multiple tiers within the Lookout Personal App. Each tier offers increased access to Lookout security features. The information required to provide these services may vary and is listed in this document to help you understand what information we collect directly from you, from your device and how we use this information. Details regarding product features for the Lookout Personal App for iOS and Android devices can be found here https://www.lookout.com/uk/products/personal/ios and https://www.lookout.com/uk/products/personal/android.

1. We Collect Information From You to Provide You with Lookout Services

When we collect your information, we store it and associate it with your account unless otherwise noted. We take your privacy very seriously and will only use and disclose this information as described in this Privacy Policy.

Some of our products are standalone products, and collect only limited information or no information at all. Feature availability will vary by product, and country. Therefore, not every section of this Privacy Policy will apply to these products.

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

Please note, our purpose in collecting application data and security scan data is to provide you with protections to help keep you and your data safe. This is also to optimise and improve our Lookout Services.

Lookout collects data about your device, which includes make, model, OS type and revision, as well as what applications have been installed. This data is de-identified and is combined with the de-identified data from other customers to produce popularity of devices in applications by region. This data will remain de-identified to ensure personal data privacy. Combining customer data in a secure and confidential way helps Lookout to better understand current security threats. This also helps to improve the Lookout Security features and services. We may also share reports resulting from this data analysis publicly, in order to help others understand mobile threats and gain insights into particular mobile application behaviour.

## 2. Information Lookout Collects for the Lookout Basic Personal App

### a. Registration Information

To create an account, you must provide an email address and a password.

### b. Device Information

When you use Lookout Services, our servers record certain information about your mobile device. This information may include an equipment identifier (e.g. IMEI, subscriber identifier (e.g. IMSI), device name, mobile phone number, device type and manufacturer, operating system type and version, wireless carrier/operator, network type, country of origin, Internet Protocol ("IP") address, and the dates and times of your requests. We also collect information about the applications on your device in order to conduct scans and to download copies of scanned application files. This may include downloading a copy of part or entire copies of application files on your device if we encounter an application that we have not previously analysed. We may also collect information about how applications behave on your device (e.g. whether an application is sending premium-rate text messages that may charge money to your phone bill) and the network services with which your applications communicate, in order to determine if any applications are behaving maliciously (e.g. whether an application is talking to a server known to host phishing websites). Each time Lookout performs a scan, we collect information that describes what application files are identified by the scan as potentially undesirable. Lookout then provides recommended choices for remediation of those files (e.g. uninstall or ignore).

We use the information described above to provide our services, and support if needed. We also aggregate information about mobile threat analysis. Information maintained in aggregate is de-identified to ensure an individual cannot be identified.

To find out more about Lookout mobile threat analysis go to https://www.lookout.com/why-lookout.

### c. Location Information

Some features we offer work better if we can locate your mobile device. With your consent, which is provided during initial registration, Lookout may collect location information in two ways. We may receive it directly from your mobile device, or, in some situations, we may receive location data from cell tower or Wi-Fi hotspot information. We may use third-party service providers to translate that information into usable location information. To prevent location data from being shared go to your mobile device settings and turn off location services.

### d. URLs

To provide the Safe Browsing service, we may transmit the URLs you receive or visit on your phone to a Lookout-provided or third-party service to determine if those URLs are unsafe (e.g. if the URLs contain phishing attacks, malware or exploits). If a URL you visit is determined to be unsafe, we store a record of the unsafe URL. We use the record of unsafe URLs you visit (1) to provide you with a notice that the URL you attempted to reach is unsafe (e.g. when you log in to the Lookout website or via email) and (2) to improve our product and conduct analysis. If you do not want us to record the unsafe URLs you visit, you may turn Safe Browsing off; all other Lookout features will continue to function.

## 3. Features Offered in the Lookout Personal App

### a. Security

Lookout's Security features, which are available on different platforms, help protect your device from cybersecurity threats. Information required to support these features is collected when you use the Lookout App. Details about this information are provided in the Device Information section of this document.

Lookout's Security features, which differ by platform, provide security by various means which include scanning for malicious apps and files and detecting an out-of-date OS. More information on Lookout's predictive security technology can be found at www.lookout.com. Automatic scans of your device may occur periodically to collect details about the applications, device and operating system files on your device. Lookout will gather the results of scans performed by our services and the most current security disposition of the device. In addition, regular updates of threat definitions will be performed. These activities help to protect your mobile endpoint by allowing the Lookout App to detect and address threats on your mobile device. This feature can be turned on or off via the Lookout App Settings.

### b. Missing Device

Lookout's Theft Protection features include Missing Device capabilities such as the ability to Locate and Scream your device remotely from your Personal account at lookout.com. The Signal Flare feature will help you locate your phone near its last known location if you lose it and its battery dies. If you have enabled Signal Flare, it collects location information and sends it back to Lookout when your battery is running low. We save the phone's location to lookout.com at the time we receive the low battery alert. This feature can be turned on or off via the Lookout App Settings.

When you activate the Missing Device features, your browser will send location information to third-party map providers (e.g. Google Maps) in order to display a map of the location within your Personal account at

lookout.com. When activating this feature, we track the device's location for several minutes in order to provide an accurate location of your device for you. This information is retained in your account history and may be deleted by you at any time, from your account settings. If you choose to delete this information or disable your account, Lookout de-identifies this data so that it is no longer associated with your personal data.

### c. Backup (Contacts)

Lookout Backup allows users to back up their contacts. This information will be transmitted to servers using an encrypted protocol and stored in the Lookout Cloud. Information can be accessed or deleted by logging into your account at Lookout.com. This feature can be turned on or off via the Lookout App Settings.

### d. Multiple Device Support

Multiple Device Support links multiple devices to one master account that controls the Master Account owner's device as well as certain features of devices associated with the Master Account. Master Account owners have control over some functions of the additional devices. For example, in a multiple device account, a user may locate or access backup data on any devices enrolled under the same account.

## 4. Information Lookout Collects for our Premium Services in the Personal App

### a. Information Collected When Upgrading to Premium Services

Lookout collects the same information stated in the Lookout Basic Personal App; registration information, device information; location information (if necessary). In addition to this information, Lookout will also collect payment information to allow you to access premium features.

### b. Payment Information

If you purchase a Premium or Premium Plus Lookout Service subscription directly from us, we use a third-party payment processor to collect your credit card information including your credit card number, expiry date, security code and other applicable billing information. Our third-party vendor will use this information to bill you for services. Lookout will have information regarding your Premium and/or Premium Plus account. This information will include the amount you paid and the method of payment. We will not have your credit card or bank information, this information remains with the third-party payment processor.

If you purchase the Lookout App from an App Store or through your Carrier plan your payment information will be managed by that App Store or Carrier. Payment does not go to Lookout. Your payment could be processed in various ways. Lookout has contract agreements in place with our Partners to ensure that you

receive the expected Lookout Mobile App performance. In order to provide our services to you, the App Store will send Lookout confirmation of your purchase. Carriers may share your phone number, subscriber ID, SKU and other non-financial information. The App Store and your Carrier will not share credit card or billing data. For additional information, please refer to your App Store or Carrier's payment processing policies and procedures.

### c. Theft Alerts Data Collection

When Theft Alerts is activated a photo is taken. The picture and location data (GPS location) are stored briefly on our servers so we can send you an email with the picture and a map of your device's location. The picture is then deleted from our server. We send the email to the address associated with your account so remember to keep your email address up to date in your account settings. We use information about Theft Alert's activities on your device to study, optimise and troubleshoot our products.

### d. Safe Browsing

Safe Browsing is a feature designed to identify and warn you of unsafe URLs so that you can choose to avoid loading them. Safe Browsing is available when you have allowed the app to run a local VPN. Using the VPN, the Safe Browsing feature scans URLs that are being accessed by your device via browsers and apps. URLs visited are anonymised and sent to the Lookout Cloud to perform security scans. URL paths are the only data related to your browsing activity that is sent to Lookout. Lookout does not collect browsing history or any other personal information.

## 5. Features Provided with the Lookout Premium Service

In addition to the basic features described above, Lookout Premium customers will gain access to new features and feature enhancements.

### a. Missing Device

Premium subscribers to Lookout receive additional capabilities in the Missing Device feature. The ability to Lock and Wipe the device remotely is provided from your Personal account at lookout.com.

### b. Theft Alerts

Theft Alerts is a Premium feature within Theft Protection. Theft Alerts allows you to locate your phone when lost. When these features are enabled, an email will be sent to you on selected events (e.g. Airplane Mode enabled) with the location of your device. On Android devices, the email includes a photo of the person who

may have stolen it using your device's camera and location features to help you figure out where your device might be (and who might have it) in the event that your device is lost or stolen.

You can view the location of your device by logging into your account on Lookout.com. These features will use the location data of your device, email and phone number you provided to Lookout from the device and will help you to recover your phone in the event it is lost.

### c. Backup (Call Logs and Photos)

Backup of Call Logs and Photos is supported for Premium subscribers. You can then access your photos through your Personal account on Lookout.com. Your photos and backed-up data can be deleted from your Lookout account at any time.

### d. Safe Browsing

Safe Browsing is a feature designed to identify and warn you of unsafe URLs so that you can choose to avoid loading them. Safe Browsing is available when you have allowed the app to run a local VPN. Using the VPN, the Safe Browsing feature scans URLs that are being accessed by your device via browsers and apps. URLs visited are anonymised and sent to the Lookout Cloud to perform security scans. URL paths are the only data related to your browsing activity that is sent to Lookout. Lookout does not collect browsing history or any other personal information.

### e. Safe Wi-Fi

With Safe Wi-Fi, Lookout analyses your Wi-Fi connection for unusual activity indicating the network is unsafe or under attack and alerts you. Safe Wi-Fi helps prevent attackers from accessing your personal data on your mobile endpoint.

### f. Breach Report (Available in English only)

With Breach Report, Lookout can alert you to relevant breaches with clear and simple actions you can take to protect yourself. You can customise alerts to be specific to companies or industries and you will also receive recommendations on what actions to take to protect your data and identity.

### g. How to Turn Features Off

If you choose, you can turn features off using the Lookout settings. For issues and enquiries please contact support@lookout.com.

## 6. Information Collected with Lookout Premium Plus (US only)

The information we collect will depend on the types of Premium Plus identity protection products you enrol in. This information is required in order to verify your identity, provide you with the requested Identity Protection Services, and charge you the agreed-upon fees. Communicating your information to third parties (such as identification verification companies, consumer reporting agencies, credit bureaus, payment validation companies, law enforcement agencies, and others) is required in order to provide those services to you. We may provide this information to our third-party service providers who assist us in providing you with identity protection services, or allow these service providers to collect certain information directly from you. These service providers may in turn provide your data to third parties for the purposes of providing you with the services requested. We and/or our service providers may also provide you with monitoring and alerts and obtain information and reports about you (or about others that you have enrolled) in order to provide the Identity Protection Services, including address history, name, alias and other reports. We require that our service providers use data collected from you only for the purposes of providing services through the Lookout App Premium Plus Product. If you upgrade to a Premium Plus Subscription that includes identity theft insurance, we will use your information to provide you with assistance and applicable insurance coverage if your identity is compromised.

If you enrol in Premium Plus, the Lookout App may request your contact information (such as name, address, phone number and email address); private information (such as driving licence number, social security number, passport number, or other identification number); financial information (such as bank account, debit and credit card numbers); medical insurance number; and other personal data about you (or other people you enrol in the service). For additional information or updates go to the Product section at Lookout.com.

## 7. Features Provided with Premium Plus (US only)

In addition to the basic features (Missing Device, Security and Backup) and premium features (Theft Alerts, Safe Wi-Fi, Breach Report, Photo Backup), Premium Plus users will receive Identity Protection which includes Identity Monitoring, Identity Insurance and Restoration.

### 1. Identity Monitoring

By upgrading to Lookout Premium Plus you will be provided with services to help protect your identity and personal information.

**a. Cyber Watch**

Cyber Watch will monitor the internet for your private information and provide alerts and recommended actions if your personal information is exposed.

**b. Social Media Watch**

Social Media Watch monitors the privacy of your personal information on social networks and sends you alerts on inappropriate posts.

**c. SSN Watch**

SSN Watch will send alerts when new names or addresses get tied to your Social Security Number.

### 2. Insurance and Restoration

Lookout can help to take care of your headache and hassle of restoring your identity if it's stolen.

### a. Identity Theft Insurance

The Lookout Premium Plus provides coverage for legal fees, lost wages and other expenses associated with recovering your stolen identity.

### b. Restoration Assistance

Lookout provides support from Identity Restoration Experts 24/7 to help recover your identity if gets stolen.

### c. Lost Wallet Recovery

Lookout will help you cancel and replace bank cards, IDs and other contents of your wallet if it is lost or stolen.

### 8. Mobile Operator Customer Care for KDDI Customers

If your mobile operator participates in our Mobile Operator Customer Care programme, you can call your mobile operator to find and secure your phone or tablet if it is lost or stolen.

In order for Lookout to deliver provide customer services, we will need information about you and your device. The Customer Care Web Application will collect your phone number, if available, and information about the type of device and operating system you are using to ensure that customer service representatives accurately identify and manage the remote functions on your device.

Lookout will use your information to inform the customer service representative so they can deliver the

expected level of customer service.

The Customer Care Web Application enables mobile operators and their customer service representatives to perform remote functions on your device at your request, including:

- Locating the device
- Locking the device
- Wiping the device
- Activating a loud siren (Scream)
- Sending a message to the device.

Customer service representatives may perform such functions only at your request and with your prior consent.

To protect users' privacy, whenever a customer service representative executes any of the above functions, Lookout notifies you via your email on file. Customer service representatives do not have access to nor control over any user data backed up via Lookout's mobile application.

## 9. Data Analytics – How We Use The Information We Collect From your Mobile Endpoint Device

We may use the results of our data analysis to send you relevant content, suggest new features, products and/or services that can enhance your experience with Lookout Services. We do not link the information we store within the analytics software to any Personal Data you submit within the mobile app. Also, information maintained in aggregate is de-identified to ensure an individual cannot be identified

In addition to using the information you provide to us and the information we collect from your mobile endpoint device to deliver Lookout services, we also use the information collected from your device to perform data analytics. These analytics provide important information which helps to improve the features and usability of our products. We analyse information such as how often you use the Lookout application on your mobile endpoint device, the events that occur within the Lookout application on your mobile endpoint device and where the Lookout application was downloaded onto your mobile endpoint device. We also use this information in aggregate to perform analysis on known and new mobile threats.

## 10. Your Use of Lookout's Website and Mobile Website and Information We Collect

When you use the Lookout website from your computer or mobile endpoint, Lookout may collect information voluntarily from you to improve your user experience. Lookout may also use analytics services in the background to measure how people use our website and emails so that we can improve our products and services as well as provide more relevant content to you. Analytics services on our website and mobile website may work by embedding invisible images that are associated with unique identifiers on our site, by using cookies or other local device storage or by using web beacons, web bugs, clear GIFs and similar tracking technologies.

### a. Content & Promotions

We may ask for your email address and other contact information while you are visiting our websites to provide you with access to various Lookout content, such as whitepapers, videos or other research materials. We may also ask you to participate in surveys, contests, promotions or sweepstakes. We may request your feedback regarding your experience with the Lookout services and products. Your contact information will be used to provide you with additional information on products and services from Lookout or our business partners. You can choose not to receive such marketing communications by clicking on the unsubscribe link in our emails, as further described below.

### b. Social Media Features

Our website includes social media Features ("Features"), such as the "like" button or interactive mini-programs that run on our site. If you use these Features, they will collect your IP address, which page you are visiting on our site, and set a cookie to enable the Features to function properly. Features may be hosted by a third party or hosted directly on our site. Your interactions with these third-party Features are governed by the privacy policy of the company providing the Feature, not by Lookout's Privacy Policy.

## 11. Lookout Website Cookie Policy

#### 1. Types of Cookies

Like many online services, we use cookies and other tools to collect and analyse information about you and your usage of our products and services. We use these technologies to deliver relevant content regarding Lookout's products and services. Cookies are small data files that we store on your computers or device. For details, see aboutcookies.org.

**2. How We Use Cookies**

We use “session” cookies to keep you logged in while you use our services, to better understand how you interact with our services, and to monitor aggregate usage and web traffic information on our services. Session cookies disappear when you log out and close your browser. We also use “persistent” cookies to recognise you when you return to our services. Persistent cookies can stay on your computer for a longer period of time than session cookies do. We also use “analytical” cookies. They allow us to recognise and count the number of visitors and to see how visitors move around our services and how they’re using them. This helps us to improve the way our website works, for example by making sure users are finding what they need easily. Finally, we may use other standard technologies, such as web beacons, web bugs, clear GIFs, and local storage, to analyse, collect and aggregate data about your use of our products and services.

**3. Cookies From Third Parties**

We believe it is important for you to know exactly what third-party cookies we use on our website and services. Below is a list of the third-party cookies that we use, which may collect Personal Data about your online activities over time and across third-party websites or online services. As we develop and improve our services, we may use other third parties and will update this list accordingly. We have also included a link to the privacy policy governing the third-party cookie.

- Google Analytics – These cookies allow us to see how you use our website and mobile application so that we can improve your experience. We encourage you to read the Google Privacy Policy. If you don’t want data reported by Google Analytics, Google permits you to opt out by installing the Google Analytics Opt-out Browser Add-on.
- Google AdWords – These cookies allow our vendors to serve ads based on your past visits to our sites and for remarketing purposes. Google may use this cookie and other tracking technology to show you our ads across the internet. Google permits you to opt out of Google's use of these cookies by visiting Google's Ads Settings.
- Marketo – These cookies help us track your visits to our website and enable us to create an engaging marketing experience for you. We also use Marketo cookies to understand your interaction with the emails we send you, and to ensure we’re sending you relevant information. For example, Marketo cookies let us know whether our emails have been viewed, and which links are clicked. You can read the Marketo Privacy Policy here.
- Social Media Features – Our website includes social media features, like the recommend button or interactive mini-programs that run on our site. If you use these Features, they will collect your IP address, which page you are visiting on our site, and set a cookie to enable the feature to function

properly. Features may be hosted by a third party or hosted directly on our site. Your interactions with these features are governed by the privacy policy of the company providing the feature, not by Lookout's Privacy Policy.

- Mixpanel, Braze and mParticle – These cookies allow us to analyse and aggregate data regarding your use of our mobile application. We encourage you to read the MixPanel Privacy Policy, Braze Privacy Policy and mParticle Privacy Policy.

## 12. Legal Basis for Using Your Information

The legal basis for using your information as set out in this Privacy Policy is as follows: (a) Use of your Personal Data is necessary to perform our obligations under any contract with you (for example, 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 the performance of a contract, use of your information is necessary for our legitimate interests or the legitimate interests of others (for example, to ensure the security of the Lookout Services, operate and market the Lookout Services, ensure safe environments for our personnel and others, make and receive payments, prevent fraud and to know the customer to whom we are providing the Lookout Services). Some processing is done to comply with applicable law.

In some cases (such as for some of our marketing activities), we may process your Personal Data based on consent.

In addition to the specific uses described above, we also use your information in the following manner:

### a. We Use Your Information to Provide, Improve and Promote our Services

We use your information to provide you with a better service, to improve our products and services, to promote our services and to develop new services. For example:

- If you fill out a survey or email Lookout for support, we may retain that information in order to provide you with support and to improve our services.
- Where available, Lookout may use client device information to let you know you need to update your operating system.
- We may send text messages to your phone to communicate with your device.
- We may use your email address or mobile number to send privacy or security-related notices and notify you of major Lookout services changes.

- We may use your email address or mobile phone number to communicate about product announcements and special promotions from Lookout or our business partners, or to administer participation in special events, surveys, contests and sweepstakes.
- We may use your information to conduct market research and engage in joint promotional activities with companies that have products that can add value to Lookout products or services (for example, with mobile operators).

### b. We May Disclose Your Information in Accordance with the Law

Like other companies, we may disclose your information consistent with the law to, for example: (i) comply with a law, regulation, or legal process (including to meet national security or law enforcement requirements); (ii) protect the safety or security of any person, entity or facility; (iii) address potential violations of our Privacy Policy or Terms of Service; (iv) investigate fraud, security, or technical issues; or (v) protect Lookout's or a third party's rights or property, our employees, users and the public.

We strongly believe that you have a right to know if we are required by law to disclose your information. As such, before we disclose your Information in response to a law enforcement request (for example, a subpoena or court order), we will notify you at the email listed in your account, unless (a) we are prohibited from doing so or (b) in emergency cases where notice could create a risk of injury or death, or the case involves potential harm to minors. Furthermore, nothing in this Privacy Policy is meant to limit any legal defences or objections that you may have to a third party's, including the government's, request to disclose your information.

### c. We Share Your Information to Provide or Improve Our Services

We share your information with other members of our corporate family, or with third parties to provide or improve our services. For example:

- We may share your information with third-party service providers of products and services integrated with our software that need to know your information to fulfil your product or service requests (for example, to map your location, send you an SMS or provide you with identity protection services), support our products and services, or analyse data for product performance and product improvement purposes.
- We may share your information with mobile operators who participate in our Mobile Operator Customer Care programme to enable them to assist you directly with Lookout Missing Device features, such as remote locate, lock, wipe, or Scream through our Customer Care Web Application, at your request.

- We may share your information to perform accounting, auditing, billing reconciliation, and collection activities.
- We may share your information with our affiliates, resellers or other third-party service providers that are working with Lookout (for example, mobile operators and MDM providers) to ensure proper delivery of your purchase and related support services, perform business-related functions, and provide you with information about products and services.

## 13. Your Data Could be Included in Security Reports

For data analysis we de-identify, aggregate and summarise data that may include some of your data. We may disclose your Information with your consent. We may also share your personal data with third parties when we have your consent to do so.

## 14. Your Choices

### a. You Can Access and Update Your Settings

Your Lookout Account on our website and/or the Lookout 'Settings' page on our mobile application allow you to update or modify certain settings that affect what data is shared with us (for example, by disabling backups of certain types of data). To protect your privacy and security, we require your username and password in order to verify your identity before granting you account access or making changes. If you wish to correct or delete inaccuracies within your Personal Data, or to request access to any personal data we obtain about you, please contact us at privacy@lookout.com. We will respond to your request to access 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.

### b. Email Opt-Outs

You may opt out of receiving promotional communications from Lookout by using the unsubscribe link within each email. Although opt-out requests are usually processed immediately, please allow ten (10) business days for a removal request to be processed. Even after you opt out from receiving promotional messages from us, you will continue to receive transactional and product-related messages from us regarding Lookout Services. You can opt-out of some of these notification messages in your account settings.

### c. Personalised Advertisements

You may be able to opt out of receiving certain personalised advertisements from companies who are

members of the Network Advertising Initiative or who subscribe to the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. Please visit the Network Advertising Initiative Consumer Opt-Out Page or the Digital Advertising Alliance Opt-Out Page to opt out directly from providers who participate in those programmes. Lookout does not control or operate these tools or the choices that advertisers and others provide through these tools.

**d. Location**

When you delete location data through your account dashboard on Lookout.com, it is no longer linked to your account and is de-identified on our application production systems.

## 15. Data Retention Policy

Our policy is to retain Personal Data only as long as reasonably necessary to provide our products and services to you or as otherwise required for legal compliance purposes. We may delete your data if your account is inactive and as otherwise provided in our Terms of Service.

## 16. Information Posted to Our Blog and Community Forum Is Public

If you comment on our blog or other public forums, you should be aware that any information you submit there can be read, collected or used by other users of those blogs, and could be used to send you unsolicited messages. We are not responsible for the information you choose to submit in these blogs or for any content you receive as a result of sharing such information.

## 17. We Take Security Seriously

Lookout is a security company, and securing your data is important to us. Lookout uses commercially reasonable physical, managerial, and technical safeguards to ensure appropriate technical and organisational measures. For example, we use a combination of firewalls, authentication, physical security, and other safeguards to protect your account and your data. When you enter sensitive information (such as credit card number or location-based information) on our website, within the Lookout app, or in our order forms, we encrypt the transmission of that information using secure socket layer technology (SSL). We also perform third-party penetration tests to harden our systems from attack. Lookout takes every reasonable effort to implement controls to protect against complex technological threats and other criminal threats, as well as to guard against negligent employees.

Because no method of transmission over the internet or method of electronic storage is 100% secure, we cannot ensure or warrant the security of any information, data or content that Lookout receives on your behalf

to operate the Lookout services, or that you transmit to Lookout. All such receipt or transmission of your information is provided under your own free will and at your own risk. We cannot guarantee that such information will not be accessed, disclosed, altered or destroyed by breach of any of our physical, technical or managerial safeguards

If Lookout learns of a security breach, we will attempt to notify you electronically so that you can take appropriate protective steps. Lookout will also post a notice on the Lookout services if a security breach occurs. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.

## 18. You Are Responsible for Maintaining the Accuracy and Confidentiality of Your Email Address and Password

You are responsible for maintaining the secrecy of your password at all times. We recommend a strong password that you do not use with other services. If you believe your password has been compromised, please change your password immediately via the Lookout website, or contact us at support@lookout.com for assistance. You are responsible for ensuring that the email address associated with your account is accurate. We use that email to contact you about service updates, changes to our policies, and account activities such as requests for your information or locate attempts on your device. Lookout is not responsible for Personal Data transmitted to a third party as a result of a user providing an incorrect email address.

## 19. Notice to California Users

### a. Do Not Track

Do Not Track is a privacy preference that users can set in their web browsers. When a user turns on the Do Not Track signal, the browser sends a message to websites requesting them not to track the user. For information about Do Not Track, visit www.allaboutdnt.org. At this time, we do not respond to Do Not Track browser settings or signals. In addition, some of our third-party services providers may use standard technology, such as cookies, pixel tags and web beacons, to collect information about your internet activities. You may be able to disable certain third-party cross-site tracking as described in the “Your Choices” section above.

## 20. International Visitors, the Privacy Shield and GDPR

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 Lookout 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. Lookout has certified with the Privacy Shield framework as set forth by the US Department of Commerce regarding the collection, use and retention of Personal Data from EU States and Switzerland. The Privacy Shield Principles lay out a set of requirements governing participating organisations' use and treatment of Personal Data received from the EU and Switzerland. By joining the Privacy Shield, participants make a commitment to comply with these Principles that is enforceable under US law. Lookout has certified that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access and enforcement for such Personal Data. To learn more about the Privacy Shield, view a list of entities who have current certifications under Privacy Shield, or view Lookout's certification, please visit http://www.privacyshield.gov.

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 privacy@lookout.com or by the postal address set forth under "Contact Us if You Have Any Questions or Concerns". We will work with you to resolve your issue.

If you are a resident of the European Union 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 elect to arbitrate 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 US 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. Each party shall be responsible for its own legal 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 US Federal Trade Commission (FTC).

In addition to the rights granted under the section above entitled, "You Can Access and Update Your Privacy Settings", some international users (including those whose information we collect under the Privacy Shield)

have certain legal rights to access certain information we hold about them and to obtain its deletion. To exercise those rights, these users may contact us at privacy@lookout.com with their request.

The European Union has taken a step to protect the fundamental right to privacy for EU residents with the General Data Protection Regulation (GDPR), which will be effective from 25 May 2018. Any organisation that works with EU residents' Personal Data in any manner, has obligations to protect the data. Lookout takes every commercially reasonable effort inclusive of recommended technical and organisational measures to comply with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR").

These efforts include:

**Identifying Personal Data** – Each Lookout service requires a different level of Personal Data collection, usage, storage and disposal. Defining the scope of Personal Data for each of these services and documenting the various sources of data provides visibility into what Personal Data we obtain and allows Lookout to appropriately manage and protect this critical asset.

**Providing Visibility and Transparency** – Lookout provides transparency and access to Personal Data by responding to customer requests in a timely manner consistent with GDPR requirements. Requests can be submitted by contacting support@lookout.com. Personal data can be viewed and updated by accessing your personal Lookout web portal.

**Ensuring data integrity and security** – To maintain data integrity Lookout manages access to customer data through strict access controls. Lookout also implements appropriate security measures by encrypting Personal Data while in transit and at rest.

## 21. Users Under 16

Because Lookout provides services to an international customer base, in order to comply with both US and EU legal requirements pertaining to both Chapter 91 – Children's Online Privacy Protection Act and Article 8 Conditions applicable to child's consent in relation to information society services of the GDPR, Lookout does not knowingly collect or store any Personal Data about children under the age of 16 unless they are part of a Multiple Device Plan purchased by a parent who consents to such collection and storage as described in the Lookout Terms of Service. If you believe a child is using this service without parental consent, please contact us at privacy@lookout.com.

## 22. We Are Not Responsible for Content on Third-Party Websites

Our site contains links to other websites. When you click on one of these links, you leave Lookout's website and go elsewhere. Lookout does not accept liability for misuse of any information by any website controller to

which we may link. We encourage you to read the privacy statements of these linked sites, which may differ from ours. In addition, if you take advantage of an offer from one of our partners, you may be providing information directly to that partner. We encourage you to review the privacy statements of these partners, as we are not responsible for the privacy practices of any partners or linked sites.

## 23. Change in Control

In the event that Lookout is involved in a bankruptcy, merger, acquisition, reorganisation or sale of assets, your information may be sold or transferred as part of that transaction.

## 24. We Post Updates on Our Website Whenever This Policy Changes

This Privacy Policy may be revised to keep pace with changes in our products and services and laws applicable to Lookout and you. If we make material changes to this policy, then we will notify you in our application, here on this website, by email, or by means of a notice on the Lookout home page. Please note that your continued use of our services means that you agree with, and consent to be bound by, the new Privacy Policy. If you do not wish your information to be subject to the revised Privacy Policy, you will need to close your account.

## 25. Contact Us if You Have Any Questions or Concerns

Please contact our Data Privacy Officer at privacy@lookout.com, or by post to Lookout, Inc., Attn: Michael Musi, Data Privacy Officer, One Front Street, Suite 3100 San Francisco, CA 94111, with any questions or comments about this policy. Residents of the EU may also make contact by sending enquiries to the attention of Mr G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Netherlands.