
Lookout, Inc.

Privacy Notice

Effective Date: 1/1/2020

INTRODUCTION 2

1. INFORMATION WE COLLECT 2

2. HOW WE USE YOUR INFORMATION 3

3. HOW WE DISCLOSE YOUR INFORMATION..... 3

4. YOUR CHOICES 4

5. USE OF COOKIES BY LOOKOUT 4

6. DATA RETENTION 5

7. SECURITY 5

8. USERS UNDER 16..... 6

9. INTERNATIONAL DATA TRANSFERS..... 6

10. ADDITIONAL TERMS FOR CALIFORNIA RESIDENTS 6

11. ADDITIONAL TERMS FOR EUROPEAN ECONOMIC AREA (“EEA”) RESIDENTS 8

12. CONTACT US IF YOU HAVE ANY QUESTIONS OR CONCERNS 9

Introduction

Lookout, Inc. (“**Lookout**” or “**us**” or “**we**”) provides this Privacy Notice (the “**Notice**”) to inform you of our practices regarding the collection, use and disclosure of information we receive from users of the lookout.com website, any other Lookout sites that link to this Notice, other Lookout events such as trade shows or sponsored events (collectively, the “**Site**”).

Except where explicitly provided otherwise herein, this Notice applies to information provided or collected through the Site, and other information collected by Lookout offline. Any information collected from you from the use of one of our applications will be subject to a separate privacy notice. Note that Lookout’s applicable terms of service for our services may contain additional notices and terms that apply to our collection and use of data and metadata in connection with your use of those services.

This Notice may be updated from time to time. We will notify you of any material changes by posting the new Notice on the Site. You are advised to consult this policy regularly for any changes.

1. Information We Collect

Lookout may collect the following categories of information, some of which you may voluntarily provide, from your use of the Site:

- **Identification Data**, including your name, title, and job title.
- **Contact Data**, including your phone number, address, and email address.
- **Cookie and Device Data**, including information about your visit of our website, IP address, device identifier, browser type and version, operating system and network, location and time zone setting, and other similar tracking technology as further explained below.
- **Event Registration Data**, including Identification Data, Contact Data, and other information you provide to us when you access various Lookout content, such as whitepapers, videos, or other research materials.
- **Job Applicant Data**, including Identification Data and Contact Data, resume and other data provided by you or third parties (e.g. recruiters) on our website in connection with job openings.

- **Third Party Information.** We may also collect these same categories of information through the use of our third-party marketing and content syndication vendors.

2. How We Use Your Information

We take your privacy very seriously and will only use and disclose this information for the business and commercial purposes described in this Notice. How we use your information will vary depending on the type of data as described below:

- Addressing customer inquiries – we use Identification Data, and Contact Data to address customer inquiries so that you may receive a response from us when you contact us.
- Sending relevant marketing messages and inviting you to events/seminars – we use Identification Data, Contact Data, Cookie and Device Data, and Event Registration Data to communicate with you by way of email alerts and mail to provide you with information about product announcements, and special promotions from Lookout or our business partners, to invite you to events that may be of interest to you, or to administer participation in surveys, contests and sweepstakes. You can choose not to receive such marketing communications by clicking on the unsubscribe link in our emails, as further described below.
- Improving our Site – we use Cookie and Device Data to improve the functionality and user-friendliness of our Site. 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 Site.
- Keeping our Site and IT systems and processes safe – we use Identification Data, Contact Data, and Cookie and Device data to ensure the security and confidentiality of your data, and to prevent illegal activities, including fraud, which could harm you and us.
- Recruitment – Job Applicant Data is collected and processed for purposes of screening, identifying, and evaluating candidates for positions; and record-keeping related to hiring processes. This processing is necessary in order to take steps at the request of the job applicant in the context of recruitment prior to entering into a contract and may be used as necessary to comply with legal, regulatory, and corporate governance requirements.

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.

3. How We Disclose Your Information

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

- **Third Party Service Providers and Partners.** We may share your information with third party service providers of products and services integrated with our Site that need to know your information for Site improvement purposes. We may share your information with our affiliates, resellers or other third-party service providers that are working with Lookout to perform business-related functions. We may also disclose your information to our third-party partners so they may contact you on our behalf with relevant marketing messages, which you can choose not to receive by clicking on the unsubscribe link in our emails.
- **Cookies.** To collect and analyze information regarding your usage of our Site as described in Section 5 below.
- **To Comply with Law.** 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 Notice; (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 Notice is meant to limit any legal defenses or objections that you may have to a third party, including the government's, request to disclose your information.

- **During a Change to Lookout's Business.** We may also disclose your information to an actual or potential buyer (and its agents and advisers) in connection with any actual or proposed purchase, merger, or acquisition of any part of our business, provided that we inform the buyer it must use your personal information only for the purposes disclosed in this Notice.
- **Pseudonymized and Aggregated Data.** For data analysis we pseudonymize, aggregate and summarize data that may include some of your data.
- **With Consent.** We may also disclose your information to third-parties when we have your consent to do so.

4. Your Choices

a. 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 may continue to receive transactional and product-related messages from us if you use the Lookout's products/services, in which case you can opt-out of these notification messages in your account settings.

b. Personalized Advertisements

You may be able to opt out of receiving certain personalized 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 programs. Lookout does not control or operate these tools or the choices that advertisers and others provide through these tools.

5. Use of Cookies by Lookout

Like most providers of online services, we use cookies and other tools to collect and analyze information regarding your usage of our Site. Cookies are small data files that we store on your computer or device. For details, see [online cookies information](#).

a. How We Use Cookies

We use "session" cookies to monitor aggregate usage and web traffic information on our Site. Session cookies disappear when you log out and close your browser. We also use "persistent" cookies to recognize you when you return to use our Site. 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 recognize and count the number of visitors and to see how visitors move around our Site and how they are interacting with our Site. This helps us to improve the experience on our Site. Finally, we may use other standard technologies, such as clear gifs and local storage to analyze, collect and aggregate data about your use of our Site. We use the data we collect from these tools as described below.

b. Cookies from Third-Parties

We believe it is important for you to know what third-party cookies we use on our Site. Here is a list of the third-party cookies that we currently use. As we develop and improve our services, we may use other third parties that are not listed below.

Adobe Experience Cloud — We use cookies from Adobe Experience Cloud (including Marketo, Bizible, and other Adobe products). These cookies help us track your visits to our Site and enable us to create an engaging marketing experience for you, to provide you with relevant marketing information. For example, these cookies let us know

information like which emails have been opened, and which links are clicked. You can read the Adobe [Privacy Policies here](#), Bizible [Privacy Policy here](#), and [Marketo Privacy Policy here](#).

Google Analytics and MixPanel — These cookies allow us to see how you use our Site so that we can improve your experience. We encourage you to read the [Google Privacy Policy](#) and [MixPanel Privacy Policy](#). If you don't want data reported by Google Analytics, you can install 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](#)

Greenhouse — These cookies are used to provide you with a personalized user experience when you apply for a job with us. You can read the [Greenhouse Privacy Policy here](#).

Hotjar — Hotjar uses cookies to process information including standard internet log information and details of the visitor's behavioral patterns upon visiting our site. This is done to provide you with a better experience, and to facilitate the use of certain functions. Hotjar stores this information in a pseudonymized user profile. Hotjar does not process this information to identify individual users or to match it with further data on an individual user. You can read the [Hotjar Privacy Policy here](#).

LinkedIn Insights — These cookies help us track your visits and your interactions on our Site so that we can provide with you an engaging marketing experience. They also enable us to deliver more relevant services and content on lookout.com and on LinkedIn's partner sites. You can read the [LinkedIn Privacy Policy here](#).

Oktopost - Lookout uses Oktopost for publishing to social media platforms. Oktopost enables us to publish, and track audience response. For more information, please read the [Oktopost Privacy Policy](#).

Onclusive - Lookout uses Onclusive (formerly AirPR), to manage press relations activities, and to measure reach. For more information, please contact [Onclusive](#).

ReachForce - Lookout uses ReachForce to enable us to provide a more streamlined experience on our forms, and to ensure more accurate data in our database. For more information, review the [ReachForce Privacy Policy](#).

Social Media Features — Social media features such as a "like" button may be hosted by a third party. If you use these Features, they may collect your IP address, and set a cookie to enable the feature to function properly. Your interactions with these features are governed by the privacy policy of the company providing the feature, not by our Notice.

c. How to Control Cookies

Most Internet browsers automatically accept cookies, but some browsers may permit you to change your settings or use third-party tools to disable cookies or to prompt you before accepting cookies from the websites you visit. These browsers or other third-party tools may also permit you to delete cookies you already have. Please be aware that some parts of our services may not work for you if you delete or disable cookies.

6. Data Retention

Lookout will retain your information, including your Personal Data (as that term is defined by the GDPR), only as long as reasonably necessary to use the Site or as otherwise required for legal compliance purposes.

7. Security

a. Lookout's Responsibilities.

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 organizational measures appropriate to the risk of processing your information. 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 on the Site we encrypt that information while in transit and at rest 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 Site, 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. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.

b. 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.

8. Users Under 16

Because Lookout provides services to an international customer base, in order to comply with both U.S. and E.U legal requirements pertaining to both Chapter 91 of 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.

9. International Data Transfers

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 Site 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 self-certified with the [E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield](#) framework 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, view a list of entities who have current certifications under Privacy Shield, 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.

With respect to personal information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

10. Additional Terms for California Residents

a. Personal Information.

In accordance with the California Consumer Privacy Act (“CCPA”), below is a list of the categories of Personal Information (as that term is defined by the CCPA) that we collect (whether through the Site or elsewhere), the categories of sources we collect them from, the business and commercial purposes for which the information was collected, and the categories of third parties with which we share the Personal Information.

Categories of Personal Information	Categories of Sources	Business or Commercial Purpose	Categories of Third Parties that we share the Personal Information
Identifiers, including real name, email address, phone number, and postal address	Consumer, Marketing platforms	Customer Service, Marketing, Analytics	Marketing Platforms, Sales Platforms, Data analytics providers
Employment-related information	Consumer	Recruiting	Applicant tracking provider
Information regarding a consumer’s interaction with our Site	Consumer, Data analytics providers, Marketing platforms	Operate Site, Site Improvement, Marketing	Marketing platforms, Data analytics providers
Geolocation Information inferred from IP address	Consumer	Operate Site	Operating platforms

b. Sale of Your Personal Information.

Lookout does not sell (as we understand that term to be defined in the CCPA) any of your Personal Information.

c. Consumer Rights.

In accordance with the CCPA, and subject to exceptions, California Consumers (as that term is defined in the CCPA) have the following rights:

- **Access.** You have the right to request that Lookout disclose and deliver the categories of Personal Information (as that term is defined in the CCPA) Lookout has collected about you, or the specific pieces of Personal Information Lookout has collected about you;
- **Deletion.** You have the right to request the deletion of your Personal Information in certain situations, except where the law allows a business to maintain a Consumer’s Personal Information, including where the Personal Information is necessary to perform a contract between the business and the Consumer;
- **Opt-Out.** You have the right to opt-out of the sale of your Personal Information, but as stated above, Lookout does not sell your Personal Information.
- **Non-Discrimination.** You have the right to not be discriminated against, including but not limited to the right not to be charged a different price for the services or denying you access to the services, on the basis of your decision to exercise any of your rights in this Section.

You may exercise your rights to access your information or to delete your information through two methods: (1) complete the webform accessible through <https://personal.support.lookout.com>, or (2) send a request to Privacy@Lookout.com. To verify your identity, we will send a verification email to the email address we have on file for you. If we cannot verify your identity, then we shall not disclose any specific pieces of Personal Information in response to an access request, and we shall deny your request to delete Personal Information in response to a deletion request. For requests to delete your information, Lookout shall use a two-step process where you must first, clearly submit the request to delete and then second, separately confirm that you want your Personal Information deleted. As a California Consumer, you may have an authorized agent make an access or deletion request on your behalf, provided that the authorized agent has your written permission, and you are able to verify your own identity directly with Lookout.

d. 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 service providers may use standard technology, such as cookies, pixel tags and web beacons, to collect information about your internet activities.

11. Additional Terms for European Economic Area (“EEA”) Residents

a. Legal Basis for Processing.

If you are a visitor from the EEA, Lookout is the data controller of your personal data. The legal basis for collecting and using your Personal Data as set out in this Notice will depend on the Personal Data (as that term is defined in the General Data Protection Regulation (“GDPR”)) concerned and the specific context in which we collect it. However, we will normally collect Personal Data from you only where: (a) use of your Personal Data is necessary to perform our obligations under any contract with you; or (b) 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 Site, 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 Site); or (c) we have your consent to do so (such as for some of our marketing activities). Some processing is done to comply with applicable law.

b. Your Rights.

In accordance with the GDPR, EEA residents have the rights described below. If you wish to exercise any of these rights, please contact us at privacy@lookout.com. 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.

- **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). In addition to the rights granted under the section above entitled, “You Can Access and Update Your Privacy Settings,” you may contact us at privacy@lookout.com with your request;
- **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 information;
- **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. “Explicit consent” would be required if Lookout relies on consent as the condition to lawfully process “special categories of personal data,” as defined in the GDPR.

If you 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.iamadr.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. You 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).

12. Contact Us if You Have Any Questions or Concerns

Please contact our Data Protection Officer at privacy@lookout.com, or by postal mail at Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 28 State Street, 19th Floor, Boston, MA 02109, with any questions or comments about this Notice. Residents of the EEA may also contact by sending inquiries to the attention of Mr. G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Netherlands.