Lookout, Inc.

Anwendung „Lookout for Work“

Datenschutzerklärung

Datum des Inkrafttretens: 01.04.2023

Erstellt am: 24.10.2016

Datenschutzerklärung für die Anwendung „Lookout for Work“

Lookout, Inc. („Lookout“, „wir“, „uns“ oder „unser“) ist der festen Überzeugung, dass Ihre Privatsphäre ebenso wichtig ist wie Ihre Sicherheit, daher möchten wir Sie in diesem Dokument darüber informieren, welche Daten von uns erfasst werden, um Ihr Gerät und die Sicherheit Ihres Arbeitgebers zu schützen. Lookout stellt diese Datenschutzerklärung für Unternehmen (die „Erklärung“) zur Verfügung, um unsere Informationspraktiken im Zusammenhang mit unserer Anwendung „Lookout for Work“ (die „Dienste“) zu erläutern. Diese Erklärung regelt, welche Daten im Rahmen der Installation und Aktivierung unserer Dienste auf Ihrem Mobilgerät durch Sie oder über Sie erfasst werden. Durch das Herunterladen und Aktivieren der Dienste befugen Sie uns zur Erfassung, Nutzung, Weitergabe und Speicherung Ihrer Daten, wie in dieser Erklärung beschrieben. Alle von Lookout auf andere Weise als durch Ihre Nutzung der Dienste erhobenen personenbezogenen Daten unterliegen einer anderen Datenschutzerklärung.

Möglicherweise wurden Sie angewiesen, die Dienste herunterzuladen und zu installieren, weil Sie bei einem Unternehmen oder einer Organisation beschäftigt sind, das bzw. die entweder (1) alle oder einige seine Mitarbeiter zur Installation der Dienste verpflichtet oder (2) alle oder einige seiner Mitarbeiter zur Installation einer Suite für das Mobilgeräte-Management verpflichtet, in der die Dienste enthalten sind. Bitte haben Sie Verständnis dafür, dass diese Erklärung, sofern hier nicht ausdrücklich anders angegeben, nur unsere Informationspraxis im Zusammenhang mit unseren Diensten regelt. Wenn Sie Fragen oder Anfragen zur Datenerfassung, -verwendung, -weitergabe und -sicherheit bei Ihrem Arbeitgeber („Arbeitgeber“) oder einem Anbieter für Mobilgeräte-Management („MDM-Anbieter“) haben oder dazu, welche Daten wir im Auftrag Ihres Arbeitsgebers erfassen, wenden Sie sich bitte an die eben erwähnten Parteien.

Lookout behält sich das Recht vor, diese Erklärung jederzeit anzupassen, sollten Gesetzesänderungen, Änderungen an unseren Praktiken zur Erfassung und Nutzung von Daten, Änderungen der Funktionen der Dienste oder technische und technologische Fortschritte dies erforderlich machen. Wenn wir wesentliche Änderungen an dieser Erklärung vornehmen, werden wir Sie nach Kräften darüber in Kenntnis setzen. Sollten Sie Einwände gegen die hierin enthaltenen Informationen haben, empfehlen wir Ihnen, die Nutzung der Dienste einzustellen.

Wir haben diese Erklärung strukturiert, um Antworten auf einige allgemeine Fragen zu unseren Diensten zu geben. Diese Erklärung enthält Antworten auf die folgenden Fragen:

1. **Was genau ist die Anwendung „Lookout for Work“?**
2. **Welche Daten erfasst Lookout von Ihrem Mobilgerät?**
3. **Liest oder überprüft Lookout meine E-Mails aus oder sieht Lookout meine Fotos ein?**
4. **Erfasst Lookout auch abseits meines Mobilgeräts Daten über mich?**
5. **Wann erfasst Lookout Daten von meinem Mobilgerät?**
6. **Wie nutzt Lookout die Daten von meinem Mobilgerät?**
7. **Gibt Lookout meine Daten an andere weiter?**
8. **Verkauft Lookout Ihre personenbezogenen Daten an andere?**
9. **Welche Informationen sieht mein Arbeitgeber NICHT?**
10. **Nutzen Sie meine Daten zu Marketingzwecken?**
11. **Wie schützt Lookout meine Daten und wie lange werden sie aufbewahrt?**
12. **Wo speichert Lookout meine Daten?**
13. **Welche Rechte und Optionen habe ich hinsichtlich meiner Daten?**
14. **Ich habe noch weitere Fragen. Wie erreiche ich Sie?**

1. Was genau ist die Anwendung „Lookout for Work“?

Bei der Anwendung „Lookout for Work“ handelt es sich um eine mobile Sicherheitslösung, die Mobilgeräte und Unternehmen vor Bedrohungen und Verstößen gegen die unternehmensinternen Richtlinien schützt. Lookout nutzt ein weltweites Netzwerk von über 100 Mio. Sensoren und ermöglicht eine vorausschauende Absicherung, indem es maschinelle Intelligenz zur Identifizierung von komplexen, auf Risiken hinweisenden Mustern nutzt, die menschlichen Analysten andernfalls entgehen würden. Wird eine Bedrohung erkannt, bietet Lookout den Mitarbeitern und Administratoren Behelfsoptionen wie das Deinstallieren einer App oder das Durchsetzen von Zugriffsberechtigungen.

2. Welche Daten erfasst Lookout von Ihrem Mobilgerät?

Zum Schutz Ihres Mobilgeräts und Ihres Arbeitgebers vor Bedrohungen erfasst Lookout Daten bestimmter Kategorien über Ihr Gerät. Zu diesen Daten zählen **möglicherweise** die folgenden:

- **Analysedaten**, die zur Analyse der Produktleistung auf Ihrem Gerät verwendet werden;
- **Anwendungsdaten**, einschließlich Metadaten aller auf Ihrem Mobilgerät installierten Anwendungen (einschließlich, aber nicht beschränkt auf die Namen und Versionen der Anwendungen), wobei wir unter bestimmten Umständen auch eine Kopie der Anwendung erfassen;
- **Konfigurationsdaten**, z. B. ob Ihr Gerät so konfiguriert ist, dass es den Root-Zugriff erlaubt, oder ob Hardware-Beschränkungen des Geräts aufgehoben wurden;
- **Gerätedaten**, einschließlich der Geräte- und MDM-Identifikation Ihres Mobilgeräts;
- **Firmware-/OS-Daten**, einschließlich Hersteller und Modell Ihres Mobilgeräts, bestimmte technische Einstellungen Ihres mobilen Geräts (einschließlich der Displaygröße und der Firmware-Version), den Typ und die Version des Betriebssystems auf Ihrem Mobilgerät;
- **Identifizierungsdaten**, z. B. Ihre geschäftliche E-Mail-Adresse – diese werden optional erfasst, es sei denn, Ihr Arbeitgeber nutzt die Datenschutz-Kontrollfunktion unserer Dienste;
- **Netzwerkdaten**, einschließlich Metadaten zu den Netzwerken, mit denen Ihr Mobilgerät verbunden ist (einschließlich, aber nicht beschränkt auf die SSID des Netzwerks oder die eindeutige MAC-/BSSID-Adresse der Netzwerkgeräte), und die IP-Adresse (aus der Ihr Land und Ihr geografischer Standort hervorgehen kann);
- **Daten über Webinhalte**, einschließlich URLs und Domains in Bezug auf böswillige Inhalte und Inhalte, die einer zusätzlichen Analyse bedürfen.

Bitte beachten Sie, dass die Bereitstellung der Dienste die Erfassung bestimmter Daten voraussetzt. Wenn Sie uns diese Daten nicht zur Verfügung stellen oder wir aufgefordert werden, diese zu löschen, haben Sie eventuell keinen Zugriff mehr auf die Dienste.

3. Liest oder überprüft Lookout meine E-Mails aus oder sieht Lookout meine Fotos ein?

Nein. Lookout erfasst nur Metadaten zu Anwendungen auf Ihrem Gerät und gegebenenfalls auch die Anwendung selbst, nicht jedoch Daten, die Nutzer in diese Anwendung eingeben. Da Lookout also keine Einsicht in die Daten hat, die Sie in die Anwendungen auf Ihrem Mobilgerät eingeben, erfasst, liest, prüft oder durchsucht Lookout nicht Ihre E-Mails oder Textnachrichten. Lookout erfasst weder Ihre Fotos noch Ihre Videos, kann aber solche Dateien lokal auf dem Gerät scannen, um Sie vor bestimmten Bedrohungen zu schützen, die sich in Foto- oder Videodateien verstecken.

4. Erfasst Lookout auch abseits meines Mobilgeräts Daten über mich?

Ihr Arbeitgeber kann Lookout Ihre E-Mail-Adresse zur Verfügung stellen, damit die Dienste aktiviert werden können. Wenn die Dienste in eine MDM-Lösung integriert sind und die Datenschutz-Kontrollmechanismen aktiviert sind, erfasst Lookout Ihre E-Mail-Adresse nicht. Lookout kann aber möglicherweise über die MDM auf Ihre E-Mail-Adresse zugreifen.

Wenn Sie die Dienste als Teil des Produkts eines MDM-Anbieters installiert haben, erfassen wir unter Umständen auch Daten zu Ihrer Person über diesen MDM-Anbieter, darunter gegebenenfalls Ihre E-Mail-Adresse, oder haben Zugriff darauf. Informieren Sie sich bitte beim zuständigen MDM-Anbieter über dessen Datenschutzpraktiken.

Lookout kann auch weitere Daten zu Ihrer Person erfassen, indem Sie uns kontaktieren und uns diese Informationen freiwillig zur Verfügung stellen und diese Informationen freiwillig öffentlich bekannt machen.

5. Wann erfasst Lookout Daten von meinem Mobilgerät?

Nach dem Herunterladen, Installieren und Aktivieren der Dienste beginnt Lookout unmittelbar mit der Erfassung von Daten von Ihrem Gerät, um sicherzustellen, dass es frei von Bedrohungen ist und den Richtlinien Ihres Unternehmens entspricht. Jede von Ihnen auf dem Mobilgerät installierte oder verwendete App wird von uns auf potenzielle Sicherheitsbedrohungen überprüft.

6. Wie nutzt Lookout die Daten von meinem Mobilgerät?

Wir verwenden die erfassten Daten für verschiedene geschäftliche und kommerzielle Zwecke. So ermöglichen es uns die über Ihr Mobilgerät erfassten Daten beispielsweise die Erkennung von Bedrohungen für Sie und/oder Ihren Arbeitgeber, die Verbesserung unserer Dienste und die Weiterentwicklung unserer anderen Produktangebote. Möglicherweise kombinieren wir auch Daten zu Ihrem Mobilgerät mit Daten von Dritten, um unsere Dienste zu optimieren. Diese Daten werden pseudonymisiert. Sollten die Ergebnisse unserer Analyse öffentlich zugänglich gemacht werden, dann zum Schutz Ihrer Privatsphäre und der Ihres Arbeitgebers nur in aggregierter und pseudonymisierter Form. Wie wir Ihre Daten verwenden, hängt von der Art der Daten ab und wird im Folgenden beschrieben:

- **Anwendungsdaten**. Wir verwenden diese Daten zur Bereitstellung unserer Dienste, indem wir die Dateien der Anwendungen zur Feststellung des böswilligen Verhaltens der Anwendungen scannen. Wenn wir auf Ihrem Mobilgerät eine von uns noch nicht analysierte Anwendung finden, wird unter Umständen eine Kopie eines Teils oder die gesamte Anwendung heruntergeladen, damit wir feststellen können, ob sie ein Risiko darstellt. Dies hängt jedoch von der Konfiguration der Dienste durch Ihren Arbeitgeber ab. Wie in Abschnitt 3 dargelegt, erfassen wir keine von Ihnen in die Anwendungen eingegebenen Benutzerdaten, wenn Sie eine Kopie der Anwendung herunterladen.
- **Konfigurationsdaten.** Wir analysieren die Konfigurationsdaten Ihres Geräts, um festzustellen, ob Ihr Gerät modifiziert, kompromittiert oder unsicher konfiguriert wurde, z. B. ob es infiziert, gerootet oder gehackt ist oder ob versäumt wurde, einen Zugangscode festzulegen.
- **Gerätedaten**. Wir verwenden Geräte- oder MDM-Kennungen, um Ihr Gerät mit einem Gerät in einem System eines Dritten, z. B. einer Mobile Device Management-Lösung, abzugleichen, damit wir diesem System mitteilen können, ob auf Ihrem Gerät Bedrohungen vorhanden sind.
- **Firmware-/OS-Daten.** Lookout verwendet diese Daten, um kompromittierte Firmware und Betriebssysteme zu identifizieren und Sie zu benachrichtigen, wenn ein Sicherheitsupdate für Ihr Gerät verfügbar ist.
- **Identifikationsdaten.** Wir erfassen Ihre geschäftliche E-Mail-Adresse auf optionaler Basis, um Ihnen kontextbezogene Informationen zur Verfügung zu stellen, wenn wir Ihren Arbeitgeber über Bedrohungen auf Ihrem Gerät in Kenntnis setzen. Wir werden Ihnen ohne entsprechende Einwilligung keine E-Mails zukommen lassen.
- **Netzwerkdaten.** Angreifer können Internetverbindungen, einschließlich WLAN-Verbindungen, dazu verwenden, um Daten zu stehlen, was als Man-in-the-Middle-Angriff (MitM) bezeichnet wird. Wir werden die SSID gegebenenfalls dazu verwenden, diese MitM-Angriffe zu identifizieren. Lookout kann anhand Ihrer IP-Adresse auch Ihr Land und die entsprechende Region identifizieren, jedoch wird der tatsächliche Gerätestandort (GPS) der Benutzer von Lookout weder ausgelesen, noch gespeichert oder weitergegeben. Wir pseudonymisieren Daten und aggregieren diese Informationen, um die Beliebtheit von Anwendungen nach Regionen zu ermitteln und unsere Analyse hinsichtlich mobiler Bedrohungen durchzuführen. Diese Daten bleiben zur Wahrung des Datenschutzes pseudonymisiert.

- **Daten über Webinhalte.** Lookout verwendet eine VPN-Schnittstelle zur Analyse des Datenverkehrs auf Ihrem Gerät hinsichtlich Bedrohungen als Teil unserer Safe Browsing-Funktion, um den Zugriff auf bösartige oder Phishing-Websites zu blockieren. Der Inhalt und der Verlauf Ihres Datenverkehrs wird nicht an Ihren Arbeitgeber weitergegeben, sodass Ihr Arbeitgeber nur darüber benachrichtigt wird, dass Sie auf eine Bedrohung gestoßen sind.

Gemäß der Datenschutz-Grundverordnung hängt die rechtliche Grundlage für die in dieser Erklärung dargelegten Verwendung Ihrer personenbezogener Daten von Ihrer Beziehung zu Ihrem Arbeitgeber sowie dem Anwendungsfall Ihres Arbeitgebers ab und kann Folgendes umfassen: (a) Die Nutzung Ihrer personenbezogenen Daten ist notwendig, damit wir unsere Pflichten aus Verträgen mit Ihnen erfüllen können (z. B. zur Erfüllung des Arbeitsvertrages durch den Arbeitgeber oder zu Lookouts Einhaltung der Nutzungsbedingungen, denen Sie durch den Download und die Nutzung unserer Anwendungen zustimmen); oder (b) wenn die Nutzung Ihrer Daten nicht zur Vertragserfüllung erforderlich ist, sind Ihre Daten notwendig im Rahmen unserer berechtigten Interessen oder denen des Arbeitgebers oder denen Dritter (z. B. zur Gewährleistung der Sicherheit der Dienste, für den Betrieb der Dienste, zur Schaffung einer sicheren Umgebung für unser Personal und das Ihres Arbeitgebers sowie andere Personen, zum Ausführen und Erhalten von Zahlungen, zur Betrugsprävention und zu unserer genaueren Kenntnis der Kunden, die unsere Dienste nutzen); und zur Einhaltung gesetzlicher Vorschriften wie jene, die eine angemessene Datensicherheit fordern.

7. Gibt Lookout meine Daten an andere weiter?

Da es sich um ein Produkt für Unternehmen handelt, werden bestimmte Daten an Ihren Arbeitgeber bzw. jede von Ihrem Arbeitgeber autorisierte Person weitergegeben. Im Dashboard für die Dienste erhalten Arbeitgeber oder deren autorisierte Personen Zugang zu bestimmten Informationen hinsichtlich der Sicherheit Ihres Mobilgeräts. Ihr Arbeitgeber kann unter Umständen Ihre Gerätemerkmale wie beispielsweise das Gerätemodell und den Netzbetreiber einsehen. Ihr Arbeitgeber erfährt, welche Anwendungen wir als bösartig identifiziert haben und welche gegen die geltenden Richtlinien Ihres Arbeitgebers verstoßen. Um zu erfahren, wie sich solche Verstöße gegen Unternehmensrichtlinien auf Sie auswirken können, wenden Sie sich an Ihren Arbeitgeber.

Wenn Sie unsere Dienste als Teil eines Produkts eines MDM-Anbieters installiert und aktiviert haben, werden wir den Sicherheits- und Aktivierungsstatus Ihres Mobilgeräts gegebenenfalls an diesen MDM-Anbieter weitergeben.

Eventuell geben wir Daten zu Ihrer Person an Dritte, darunter andere Gesellschaften unserer Unternehmensgruppe sowie Dienstanbieter oder Partner weiter, die in unserem Auftrag geschäftsrelevante Funktionen ausführen. Dazu können Dienstanbieter zählen, die: (a) Kundensupport, technischen Support oder betrieblichen Support leisten; (b) Aufträge abwickeln und Anfragen von Anwendern oder Arbeitgebern bearbeiten; (c) unsere Dienste hosten; (d) Datenbanken instand halten; (e) Daten zum Zweck der Produktverbesserung und -erweiterung analysieren; und (f) unser Dienste oder andere Lookout-Produkte anderweitig unterstützen oder vermarkten. Wir geben Ihre Daten eventuell im Rahmen von Vorladungen, Gerichtsbeschlüssen oder anderen rechtlichen Verfahren, die uns betreffen, weiter, oder um unsere gesetzlichen Rechte zu begründen oder auszuüben oder um uns gegen Rechtsansprüche zu verteidigen. Wenn Strafverfolgungsbehörden auf Regional-, Landes- oder Bundesebene oder ausländische Strafverfolgungsbehörden die Herausgabe von Daten verlangen, werden wir uns bemühen, Ihrem Arbeitgeber diese Anträge zur Bearbeitung vorzulegen, allerdings behalten wir uns das Recht vor, direkt auf solche Anträge mit der Herausgabe der gewünschten Daten zu reagieren, wenn wir dies für rechtlich angemessen erachten. Eventuell werden wir Daten zu Ihrer Person weitergeben, wenn wir in gutem Glauben davon ausgehen, dass dies angemessen ist, um hinsichtlich illegaler Aktivitäten, mutmaßlichen Betrugs, Situationen mit Risiko für die körperliche Unversehrtheit von Personen, Verstößen gegen diese Datenschutzerklärung, die Lizenzvereinbarung oderdie Anwendervereinbarung für die Dienste zu ermitteln, vorbeugende Maßnahmen oder Gegenmaßnahmen zu ergreifen. Die Weitergabe kann zusätzlich/alternativ erfolgen, um die Rechte und das Eigentum von Lookout, unsere Mitarbeiter, Anwender und die Öffentlichkeit zu schützen. Die Weitergabe Ihrer Daten kann unter anderem an Strafverfolgungsbehörden, Regierungsbehörden, Gerichte und/oder andere Organisationen erfolgen.

Eventuell werden wir Daten zu Ihrer Person in Verbindung mit einer Fusion, Neuorganisation, Veräußerung einiger oder aller Lookout-Vermögensgegenstände oder Finanzierung oder Übernahme aller oder einiger unserer

Geschäftsbereiche durch ein anderes Unternehmen weitergeben.

8. Verkauft Lookout meine personenbezogenen Daten an andere?

Nein. Lookout verkauft die personenbezogenen Daten (wie dieser Begriff nach unserem Verständnis im California Consumer Privacy Act definiert ist) seiner Benutzer nicht. Wie im vorstehenden Abschnitt 6 erwähnt, fassen wir möglicherweise Daten zu Ihrem Mobilgerät und Daten von Dritten zusammen, um unsere Dienste zu verbessern; diese Daten sind aber pseudonymisiert und enthalten keine personenbezogenen Daten.

9. Welche Informationen sieht mein Arbeitgeber NICHT?

Lookout gibt nur Informationen an Ihren Arbeitgeber weiter, die von diesem zur Überprüfung der Bedrohungsfreiheit Ihres Geräts und zur Einhaltung der Sicherheitsrichtlinien des Unternehmens benötigt werden. Lookout ermöglicht es Ihrem Arbeitgeber beispielsweise nicht, den Inhalt Ihrer E-Mails, Ihren Browserverlauf, Ihre Kontakte, Ihren Kalender, Ihre Textnachrichten, die von Ihnen installierten und nicht bösartigen Anwendungen oder Ihren Standort einzusehen (es sei denn, die Verwendung einer solchen Anwendung verstößt gegen eine geltende Unternehmensrichtlinie Ihres Arbeitgebers).

10. Nutzen Sie meine Daten zu Marketingzwecken?

Daten, die automatisiert über Ihr Mobilgerät erfasst werden, nutzen wir weder, um Ihnen Produkte zu verkaufen, noch geben wir Sie zu Marketingzwecken an Dritte weiter. Eventuell bündeln wir über Ihr Mobilgerät erfasste Daten, um Marktforschung zu betreiben und Einblicke in die Sicherheit und Risiken von Mobilgeräten zu bieten. In diesen Fällen sind die gebündelten Daten, die in diese Studien einfließen, pseudonymisiert.

11. Wie schützt Lookout meine Daten und wie lange werden sie aufbewahrt?

Anhand angemessener administrativer, technischer und physischer Sicherheitsmaßnahmen schützen wir Ihre Daten vor unbefugtem Zugriff, Vernichtung oder Manipulation. Diese Maßnahmen sind ausgerichtet am aktuellen Stand der Technik und an der sensiblen Natur der von uns erfassten, verarbeiteten und gespeicherten Daten.

Wir ergreifen angemessene Maßnahmen, um die unbefugte Einsicht in Informationen zu verhindern, doch da keine internetbasierte Übertragungsmethode und keine Methode der elektronischen Speicherung hundertprozentig sicher ist, können wir nicht zusichern, dass die von uns erfassten Daten nie unter Verletzung dieser Erklärung weitergegeben werden.

Wir verpflichten uns dazu, personenbezogene Daten nur so lange aufzubewahren, wie dies angemessenerweise nötig ist, um Ihnen und anderen unsere Dienste bereitzustellen, oder wie es anderweitig zur Einhaltung gesetzlicher Vorschriften erforderlich ist. Bei Inaktivität Ihres Kontos oder wenn anderweitig durch unsere Nutzungsbedingungen vorgeschrieben, können wir Ihre Daten nach 60 Tagen löschen. Daten können in Form von Kopien, die zu Backup- und Business-Continuity-Zwecken angefertigt werden, weiterbestehen. In diesem Fall sind alle ruhenden Daten durch 256-Bit-Verschlüsselung abgesichert.

12. Wo speichert Lookout meine Daten?

Lookout ist ein Unternehmen mit Hauptsitz im US-Bundesstaat San Francisco und Servern in den USA. Personenbezogene Daten von Benutzern außerhalb der USA werden in die USA übertragen. Wenn Sie die Dienste außerhalb der USA verwenden, können Ihre Daten in die USA gesendet und dort gespeichert und verarbeitet werden, weil dort unsere Server und Datenbanken betrieben werden. Außerdem können wir Ihre Daten in andere Länder senden, in denen Lookout oder unsere verbundenen Unternehmen, Tochterunternehmen und Dienstanbieter Einrichtungen unterhalten.

Eventuell weichen die Datenschutzgesetze dieser Länder von denen in Ihrem Land ab, beispielsweise indem sie weniger Schutz bieten. Bei der Übertragung und Verarbeitung Ihrer Daten ergreifen wir jedoch Maßnahmen zum

Schutz Ihrer personenbezogenen Daten gemäß dieser Erklärung und den geltenden Datenschutzgesetzen. Für Einwohner des Europäischen Wirtschaftsraums („EWR“), des Vereinigten Königreichs oder der Schweiz setzen wir diverse rechtliche Mechanismen ein, die den Schutz Ihrer personenbezogenen Daten und Ihrer Rechte gewährleisten. Dazu zählen von der Europäischen Kommission genehmigte Standardvertragsklauseln zur Übertragung von personenbezogenen Daten in Drittländer.

Lookout ist zudem gemäß den vom US-Handelsministerium herausgegebenen Rahmenwerken EU-US-Datenschutzschild und Schweiz-US-Datenschutzschild zertifiziert, die die Erfassung, Verwendung und Aufbewahrung personenbezogener Daten aus der Europäischen Union, dem Vereinigten Königreich und der Schweiz regeln. Diese Rahmenwerke wurden entwickelt, damit Unternehmen bei der Übermittlung von personenbezogenen Daten aus der Europäischen Union, dem Vereinigten Königreich und der Schweiz in die Vereinigten Staaten den Anforderungen an den Datenschutz entsprechen können. Weitere Informationen zum Datenschutzschild und unsere diesbezügliche Bescheinigung finden Sie hier: http://www.privacyshield.gov.

Als für den Datenschutzschild zertifiziertes Unternehmen achtet Lookout die Grundsätze des Datenschutzschilds hinsichtlich personenbezogener Daten aus der Europäischen Union, dem Vereinigten Königreich und der Schweiz. Gemäß den oben genannten Grundsätzen haftet Lookout in bestimmten Fällen, wenn Daten, die das Unternehmen im Rahmen des Datenschutzschilds erhält und dann einem externen Dienstanbieter, der im Auftrag von Lookout als sein Erfüllungsgehilfe auftritt, übermittelt. Die Haftbarkeit besteht, wenn beides zusammen auftritt: (i) Der Erfüllungsgehilfe verarbeitet die Daten nicht im Einklang mit dem Datenschutzschild und (ii) Lookout ist für das Ereignis verantwortlich, das den Schaden verursacht hat.

Bei Fragen oder Beschwerden zu den Datenschutzpraktiken von Lookout, insbesondere bei Fragen zum Datenschutzschild, erreichen Sie uns unter der E-Mail-Adresse oder Anschrift im Abschnitt „Ich habe noch weitere Fragen. Wie erreiche ich Sie?“. Gemeinsam mit Ihnen werden wir versuchen, das Problem zu lösen.

13. Welche Rechte und Optionen habe ich hinsichtlich meiner Daten?

Wenn Sie im EWR, im Vereinigten Königreich oder in der Schweiz ansässig sind, genießen Sie gemäß der Datenschutz-Grundverordnung („DSGVO“) möglicherweise die folgenden Rechte:

- **Recht auf Auskunft.** Sie haben das Recht, eine Kopie der von uns zu Ihrer Person verarbeiteten personenbezogenen Daten anzufordern. Wenn Sie zusätzliche Kopien benötigen, müssen wir gegebenenfalls eine entsprechende Gebühr erheben.
- **Recht auf Berichtigung.** Sie haben das Recht, die Berichtigung aller fehlerhaften oder unvollständigen personenbezogenen Daten zu verlangen, die wir zu Ihrer Person gespeichert haben.
- **Recht auf Löschung.** Sie haben das Recht, die Löschung der Sie betreffenden personenbezogenen Daten in bestimmten Situationen zu verlangen, z. B. wenn wir diese nicht länger benötigen oder wenn Sie Ihre Einwilligung (soweit vorhanden) widerrufen.
- **Recht auf Übertragbarkeit.** Sie haben das Recht, die Sie betreffenden und von Ihnen zur Verfügung gestellten personenbezogenen Daten in einem strukturierten, allgemein üblichen und maschinenlesbaren Format zu erhalten und in bestimmten Situationen an Dritte weiterleiten zu lassen.
- **Recht auf Widerspruch.** Sie haben das Recht, (i) der Verarbeitung Ihrer personenbezogenen Daten zu Zwecken des Direktmarketings jederzeit zu widersprechen; und (ii) unserer Verarbeitung Ihrer personenbezogenen Daten zu widersprechen, wenn die rechtliche Grundlage einer solchen Verarbeitung für unsere berechtigten Interessen oder die eines Dritten erforderlich ist.
- **Recht auf Einschränkung der Verarbeitung.** Sie haben das Recht, eine Einschränkung der Verarbeitung Ihrer personenbezogenen Daten durch uns unter bestimmten Umständen zu verlangen, z. B. wenn Sie die Richtigkeit dieser personenbezogenen Daten anfechten.

- **Recht auf Widerruf der Einwilligung.** Sofern wir uns bei der Verarbeitung Ihrer personenbezogenen Daten auf Ihre Einwilligung (oder Ihre ausdrückliche Zustimmung) als rechtliche Grundlage stützen, haben Sie das Recht, diese Einwilligung jederzeit zu widerrufen.

Wenn Sie eines dieser Rechte ausüben möchten, wenden Sie sich bitte an Ihren Arbeitgeber. Sofern Lookout die Funktion des für die Datenverarbeitung Verantwortlichen ausübt, können Sie sich auch über die nachstehend aufgeführten Kontaktdaten an uns wenden, um diese Rechte auszuüben. Unter angemessenen Umständen können wir die Anfrage an Ihren Arbeitgeber weiterleiten und seinen Anweisungen zur Umsetzung Folge leisten. Wir werden auf Ihre Anfrage schnellstmöglich, spätestens jedoch innerhalb von 30 Tagen, reagieren. In einigen Fällen kann es jedoch vorkommen, dass Lookout Ihnen keinen Einblick verschaffen oder nicht alle personenbezogenen Daten löschen kann, die wir zu Ihrer Person gespeichert haben.

Wenn Sie im EWR, im Vereinigten Königreich oder in der Schweiz ansässig und mit der Art und Weise unzufrieden sind, in der wir auf Ihre Bedenken bezüglich unserer Datenschutzpraktiken reagieren, können Sie im Rahmen unseres designierten unabhängigen Datenschutzschild-Regressmechanismus kostenfrei weitere Unterstützung erbitten. Weitere Informationen hierzu finden Sie auf https://www.jamsadr.com/eu-us-privacy-shield. Sie haben zudem das Recht, bei der zuständigen Aufsichtsbehörde Beschwerde einzulegen. Allerdings möchten wir Sie bitten, sich mit Ihren Bedenken zuerst an uns zu wenden, damit wir alles uns Mögliche unternehmen können, um das Problem zu lösen. In der Europäischen Union ansässige Personen haben ferner das Recht, ungelöste Beschwerden durch ein verbindliches Schlichtungsverfahren beilegen zu lassen. Vor einer Schlichtung sind jedoch folgende Voraussetzungen zu erfüllen: (1) Sie müssen Lookout kontaktieren, damit wir die Möglichkeit haben, das Problem zu lösen; (2) Sie müssen den designierten unabhängigen Regressprozess von Lookout (siehe oben) nutzen; (3) Sie müssen das US-Handelsministerium kontaktieren (entweder direkt oder durch eine europäische Datensicherheitsbehörde) und ihm ausreichend Zeit lassen, einen Versuch der Problemlösung zu unternehmen. Weitere Informationen zum verbindlichen Schlichtungsverfahren im Rahmen des Datenschutzschilds finden Sie unter https://www.privacyshield.gov/article?id=ANNEX-I-introduction. Jede Partei trägt ihre eigenen Anwaltsgebühren. Bitte beachten Sie, dass die Schiedsstelle gemäß dem Datenschutzschild nur befugt ist, einzelfallbezogene, nichtmonetäre billigkeitsrechtliche Ansprüche anzuerkennen, um hinsichtlich Privatpersonen Verstöße gegen die Grundsätze abzustellen. Lookout unterliegt den Ermittlungs- und Durchsetzungsbefugnissen der US-Verbraucherschutzbehörde FTC (Federal Trade Commission).

Gemäß geltendem Recht, einschließlich der Datenschutz-Grundverordnung und des kalifornischen Verbraucher- und Datenschutzgesetzes (Consumer Privacy Act), verfügen Sie möglicherweise über bestimmte Rechte. Wenn Sie eines dieser Rechte ausüben möchten, wenden Sie sich bitte an Ihren Arbeitgeber. Darüber hinaus können Sie auch uns kontaktieren, die Kontaktdaten finden Sie nachstehend.

14. Ich habe noch weitere Fragen. Wie erreiche ich Sie?

Sollten Sie weitere Fragen haben, empfehlen wir Ihnen, sich an Ihren Arbeitgeber zu wenden. Sie können Ihre Fragen auch direkt an unseren Datenschutzbeauftragten unter privacy@lookout.com oder per Post an folgende Adresse richten: Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA 02108. Im EWR ansässige Personen können per Post unter folgender Adresse Kontakt mit uns aufnehmen: Lookout, Inc., Attn: Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem, Niederlande.