Datenschutzerklärung für Unternehmen

Datum des Inkrafttretens:
24.10.2016
Erstellt am: 24.10.2016
Überarbeitet am: 25.05.2018
Status: Genehmigt

Inhaltsverzeichnis

Überarbeitungsverlauf

Dieses Dokument untersteht der Kontrolle von Lookout, Inc., daher dienen Ausdrucke dieses Dokuments lediglich als Referenz. Jeder Anwender muss sich eigenständig vergewissern, dass ihm die aktuelle Version vorliegt. Muss ein Teil dieses Dokuments überarbeitet werden, so ist das gesamte Dokument neu herauszugeben.

Version	Datum	Beschreibung	Eingereicht von
1.0	24.10.2016	Aktueller Entwurf auf öffentlicher Website	Marcelo Guerra
2.0	01.04.2018	Überarbeitung der Richtlinie im Einklang mit Produktangebot	Kimberly Snow

Datenschutzerklärung für Mobile Endpoint Security

Für Lookout sind Ihre Privatsphäre und Ihre Sicherheit gleichermaßen wichtig, deshalb wird in diesem Dokument erläutert, welche Daten wir erfassen, um Ihr Gerät und Ihren Arbeitgeber zu schützen. Lookout, Inc. („Lookout“, „wir“ oder „uns“ bzw. „unser/e“) gibt diese Datenschutzerklärung für Unternehmen heraus, um unseren Umgang mit Daten hinsichtlich unserer „Mobile Endpoint Security“-Produkte (das „Endpunkt-Sicherheitsprodukt“) zu erläutern. Diese Datenschutzerklärung für Unternehmen regelt, welche Daten im Rahmen der Installation und Aktivierung unseres Endpunkt-Sicherheitsprodukts auf Ihrem Mobilgerät durch Sie oder über Sie erfasst werden. Durch das Herunterladen und Installieren des Endpunkt-Sicherheitsprodukts befugen Sie uns zur Erfassung, Verwendung, Weitergabe und Speicherung Ihrer Daten wie in dieser Datenschutzerklärung für Unternehmen beschrieben.

Möglicherweise wurden Sie angewiesen, das Endpunkt-Sicherheitsprodukt herunterzuladen und zu installieren, weil Sie bei einem Unternehmen oder einer Organisation beschäftigt sind, das bzw. die entweder (1) alle oder einige Mitarbeiter dazu verpflichtet, das Endpunkt-Sicherheitsprodukt zu installieren, oder (2) alle oder einige Mitarbeiter dazu verpflichtet, eine Suite für das Mobilgeräte-Management zu installieren, die das Endpunkt-Sicherheitsprodukt enthält. Bitte beachten Sie, dass diese Datenschutzerklärung für Unternehmen nur unseren Umgang mit Daten hinsichtlich unseres Endpunkt-Sicherheitsprodukts 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 Datenschutzerklärung für Unternehmen anzupassen, sollten Gesetzesänderungen, Änderungen an unseren Datenerfassungs- und Datennutzungspraktiken, Funktionsänderungen bei unserem Endpunkt-Sicherheitsprodukt oder technische und technologische Fortschritte dies erforderlich machen. Deshalb empfehlen wir Ihnen, diese Webseite regelmäßig zu besuchen. Wenn Sie das Endpunkt-Sicherheitsprodukt trotz veröffentlichten Änderungen an dieser Datenschutzerklärung für Unternehmen weiter nutzen, akzeptieren Sie damit diese Änderungen.

Mit der Struktur dieser Datenschutzerklärung für Unternehmen möchten wir die folgenden dringenden Fragen zum Endpunkt-Sicherheitsprodukt beantworten:

1. Worum handelt es sich bei Lookout Mobile Endpoint Security?

Lookout Mobile Endpoint Security (MES) ist eine mobile Sicherheitslösung, die die Risiken eines ungeschützten Datenzugriffs über Mobilgeräte minimiert. Die Lösung liefert Einblicke in mobile Bedrohungen für Apps, Geräte und das Netzwerk, lässt sich nahtlos in vorhandene Mobilgerätelösungen integrieren und erweitert diese. Darüber hinaus sorgt ihre Bedienerfreundlichkeit auch für eine geringere Inanspruchnahme des Helpdesks. Ein weltweites Netzwerk aus mehr als 100 Millionen Sensoren macht die MES-Plattform von Lookout zu einer vorausschauenden Lösung, da maschinelle Intelligenz komplexe, auf Risiken hindeutende Muster identifiziert, die menschlichen Analysten sonst entgehen würden. Wird eine Bedrohung erkannt, bietet Lookout den Mitarbeitern und Administratoren Behelfsoptionen wie das Deinstallieren einer App oder das Durchsetzen von Zugriffsberechtigungen. Die Lösungsbereitstellung erfolgt durch eine Integration von Lookout MES mit führenden MDM-Anbietern.

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** diese:

- Hersteller und Modell des Mobilgeräts
- Bestimmte technische Einstellungen des Mobilgeräts, z. B. die Displaygröße und Firmware-Version
- Ihre IP-Adresse (kann über Ihr Land und Ihren genauen Aufenthaltsort Aufschluss geben)
- Typ und Version des mobilen Betriebssystems
- Die eindeutige Kennung des Mobilgeräts
- Gerätekonfigurationsdaten, z. B. ob Root-Zugriff erlaubt ist oder Hardware-Beschränkungen aufgehoben wurden
- Metadaten zu allen Apps auf Ihrem Mobilgerät (z. B. die Namen und Versionen der Apps)
- Metadaten zu den Netzwerken, mit denen sich das Mobilgerät verbinden kann (z. B. Netzwerk-SID oder die eindeutige MAC/BSSID-Adresse der Netzwerkgeräte)

- App-Kopien, unter bestimmten Umständen
- Daten von Tracking-Tools, zur Analyse der Leistung des Produkts auf dem Gerät
- Ihre Reaktion auf Warnungen von Lookout, dass bestimmte Apps eine Sicherheitsbedrohung darstellen können

Wenn Sie die Datenschutz-Kontrollmechanismen unseres „Mobile Endpoint Security"-Produkts in Verbindung mit einem MDM-Anbieter verwenden, erfassen wir personenbezogene Daten wie Nutzernamen und E-Mail-Adressen nicht.

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

3. Lookout erfasst Daten zu den Apps auf meinem Gerät – heißt das, Lookout liest oder prüft meine E-Mails oder sieht meine Fotos?

Nein. Lookout erfasst nur Metadaten zu Apps auf Ihrem Gerät und gegebenenfalls auch die App selbst, nicht jedoch Daten, die Nutzer in diese Apps eingeben. Da Lookout also keine Einsicht in die Daten hat, die Sie in die Apps auf Ihrem Mobilgerät eingeben, erfasst, liest, prüft oder durchsucht Lookout nicht Ihre E-Mails, Textnachrichten, Fotos oder Videos.

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

Wenn unser „Mobile Endpoint Security"-Produkt nicht im Rahmen einer Integration mit einem MDM-Anbieter installiert wird, muss jeder Mitarbeiter sein Mobilgerät mit einer bestimmten E-Mail-Adresse verknüpfen. So kann Ihr Arbeitgeber, um MES-Dienste zu ermöglichen, Lookout eventuell Ihre E-Mail-Adresse zukommen lassen. Wenn das Endpunkt-Sicherheitsprodukt von Lookout allerdings in eine MDM-Lösung integriert ist und die Datenschutz-Kontrollmechanismen aktiviert sind, erfasst Lookout Ihre E-Mail-Adresse nicht.

Wenn Sie das „Mobile Endpoint Security"-Produkt als Teil eines Produkts eines MDM-Anbieters installiert haben, werden wir eventuell auch Daten über Sie von diesem MDM-Anbieter erfassen. Informieren Sie sich bitte beim zuständigen MDM-Anbieter über dessen Datenschutzpraktiken.

Lookout darf auch andere Informationen über Sie erfassen, wenn wir sie direkt von Ihnen erhalten, indem Sie uns kontaktieren und uns diese Informationen freiwillig zur Verfügung stellen oder indem Sie Ihre Informationen Dritten wie unseren Partnern und Vermarktern geben. Mithilfe dieser Informationen werden wir Sie eventuell mit Neuigkeiten zu Lookout sowie unseren Produkten und Diensten versorgen, können Sie aber auch zu Konferenzen und anderen Veranstaltungen mit Lookout als Teilnehmer oder Veranstalter einladen.

5. Wann erfasst Lookout Daten von meinem Mobilgerät?

Wie oben beschrieben erfasst Lookout Ihre E-Mail-Adresse über Ihren Arbeitgeber, wenn das „Mobile Endpoint Security“-Produkt ohne MDM installiert wurde. Wenn das „Mobile Endpoint Security“-Produkt allerdings in Verbindung mit einer MDM-Lösung installiert wurde und die Datenschutz-Kontrollmechanismen aktiviert sind, erfasst Lookout Ihre E-Mail-Adresse nicht. Nach dem Herunterladen, Installieren und Aktivieren des „Mobile Endpoint Security“-Produkts beginnt Lookout unmittelbar mit der Datenerfassung über Ihr Gerät. 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?

Die Rechtsgrundlage für die in dieser Datenschutzrichtlinie für Unternehmen erläuterte Nutzung hängt 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 Apps 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 anderer (z. B. zur Gewährleistung der Sicherheit der Lookout-Dienste, für den Betrieb der Lookout-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 Lookout-Dienste nutzen); und zur Einhaltung gesetzlicher Vorschriften wie jene, die eine angemessene Datensicherheit fordern.

Daten, die wir über Ihr Mobilgerät erfassen, ermöglichen uns die Erkennung von Bedrohungen für Sie und/oder Ihren Arbeitgeber, die Verbesserung unseres Endpunkt-Sicherheitsprodukts und die Verbesserung unserer anderen Produktangebote. Finden wir auf Ihrem Gerät eine von uns bisher nicht analysierte App, wird unter Umständen eine Kopie eines Teils oder der gesamten App heruntergeladen und auf Risiken geprüft. Daraufhin erhalten Sie von uns die Möglichkeit, die riskante App zu deinstallieren oder das Risiko zu ignorieren. Des Weiteren erfassen wir die von Ihnen gewählte Option für die Beseitigung präparierter Dateien und Apps (z. B. Deinstallation oder ignorieren) und nutzen die erfassten Daten eventuell zur Kategorisierung des Risikoniveaus Ihres Geräts (z. B. gering, mittel, hoch).

Als Produkt für Unternehmen erfasst Lookout MES die Daten nicht nur zum Schutz Ihres Mobilgeräts, sondern auch zum Schutz Ihres Arbeitgebers.

Möglicherweise kombinieren wir auch Daten zu Ihrem Mobilgerät mit Daten von Dritten, um unsere Produkte, darunter das „Mobile Endpoint Security“-Produkt, zu verbessern. Diese Daten werden anonymisiert. Sollten die Ergebnisse unserer Analyse öffentlich zugänglich gemacht werden, dann zum Schutz Ihrer Privatsphäre und

der Ihres Arbeitgebers nur in aggregierter und anonymisierter Form.

Basiert die Datenverarbeitung durch uns auf Ihrer Einwilligung, so können Sie diese jederzeit widerrufen. Davon unberührt bleibt die Rechtmäßigkeit der Datenverarbeitung, die vor dem Widerruf Ihrer Einwilligung stattfand. Um Ihre Einwilligung zu widerrufen, wenden Sie sich an Ihren Arbeitgeber (oder gegebenenfalls an uns, unter den nachstehenden Kontaktdaten).

7. Gibt Lookout meine Daten an andere weiter?

Ja. Da es sich um ein Produkt für Unternehmen handelt, werden bestimmte Daten an Ihren Arbeitgeber bzw. jeden von Ihrem Arbeitgeber Befugten weitergegeben. Im Dashboard des „Mobile Endpoint Security"-Produkts erhalten Arbeitgeber und die von ihnen Befugten Zugriff auf bestimmte Informationen hinsichtlich der Sicherheit Ihres Mobilgeräts. Ihr Arbeitgeber sieht so eventuell auch eindeutige Gerätemerkmale wie das Modell und den Netzanbieter. Er erfährt, welche Apps wir als infiziert eingestuft haben und welche Apps gegen geltende Richtlinien in Ihrem Unternehmen verstoßen. Um zu erfahren, wie sich solche Verstöße gegen Unternehmensrichtlinien auf Sie auswirken können, wenden Sie sich an Ihren Arbeitgeber.

Wenn Sie das „Mobile Endpoint Security"-Produkt als Teil eines Produkts eines MDM-Anbieters installiert und aktiviert haben, werden wir eventuell auch Daten, die wir von Ihrem Mobilgerät erfasst haben, 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) Zahlungen abwickeln; (d) unsere Online-Dienste hosten; (e) Datenbanken instand halten; (f) Daten zum Zweck der Produktverbesserung und -erweiterung analysieren; und (g) unser Endpunkt-Sicherheitsprodukt oder andere Lookout-Produkte und -Dienste anderweitig unterstützen oder vermarkten. Eventuell geben wir Daten zu Ihrer Person weiter im Rahmen von Vorladungen, gerichtlichen Anordnungen oder sonstigen Rechtsverfahren, die uns erreichen, oder um unsere gesetzmäßigen Rechte zu begründen oder auszuüben oder uns gegen gesetzliche Forderungen zu verteidigen. Wenn Strafverfolgungsbehörden auf Regional-, Landes- oder Bundesebene oder ausländische Strafverfolgungsbehörden die Herausgabe von Informationen 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 Informationen zu reagieren, wenn wir dies für rechtlich angemessen erachten. Eventuell werden wir Daten zu Ihrer Person weitergeben, wenn wir guten Glaubens sind, dass dies angemessen ist, um hinsichtlich illegaler Aktivitäten, mutmaßlichen Betrugs, Situationen mit Risiko für die körperliche Unversehrtheit von Personen, Verstößen gegen diese Datenschutzrichtlinie, die Lizenzvereinbarung oder Anwendervereinbarung für das Endpunkt-Sicherheitsprodukt 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. Welche Informationen sieht mein Arbeitgeber NICHT?

Lookout ermöglicht es Ihrem Arbeitgeber nicht, die Inhalte Ihrer persönlichen E-Mails, den Browserverlauf, Kontakte, den Kalender oder Ihre persönlichen Textnachrichten einzusehen. Ihr Arbeitgeber hat möglicherweise bestimmte Rechte, die es ihm erlauben, diese Informationen selbst einzusehen, beispielsweise, wenn sie über ein vom Arbeitgeber bereitgestelltes Gerät oder Netzwerk übermittelt werden. Lookout wird Ihrem Arbeitgeber allerdings keinen Einblick in die Apps auf Ihrem Gerät gewähren, es sei denn, sie lassen den Verdacht aufkommen, infiziert zu sein oder gegen Unternehmensrichtlinien zu verstoßen.

9. 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 Einblick in die Sicherheit und Risiken von Mobilgeräten zu bieten. In diesen Fällen sind die gebündelten Daten, die in diese Studien einfließen, anonymisiert.

Allerdings dürfen wir die Daten, die Sie uns direkt oder Dritten wie unseren Partnern und Vermarktern zur Verfügung stellen, dazu nutzen, Ihnen Informationen über Lookout und unsere Produkte und Dienste zukommen zu lassen, darunter Konferenzen und andere Veranstaltungen mit Lookout als Teilnehmer oder Veranstalter.

10. 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 Datenschutzerklärung weitergegeben werden.

Wir verpflichten uns dazu, personenbezogene Daten nur so lange aufzubewahren, wie dies angemessenerweise nötig ist, um Ihnen und anderen unsere Produkte und 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 90 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.

11. Wo speichert Lookout meine Daten?

Lookout ist ein Unternehmen mit Hauptsitz in San Francisco und Servern in den USA. Personenbezogene Daten von Anwendern außerhalb der USA werden in die USA übertragen. Wenn Sie die Lookout-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. Lookout ist gemäß dem Datenschutzschild-Abkommen seitens des US-Handelsministeriums zertifiziert, das die Erfassung, Verwendung und Aufbewahrung personenbezogener Daten aus der EU und der Schweiz regelt. Die Grundsätze des Datenschutzschilds schreiben den Mitgliedsorganisationen vor, wie sie mit Daten zu in der EU oder in der Schweiz ansässigen Personen umzugehen haben. Im Namen des Datenschutzschilds verpflichten sich die Teilnehmer zur Einhaltung dieser Grundsätze, die unter US-Recht auch einklagbar sind. Lookout wird bescheinigt, dass es sich hinsichtlich personenbezogener Daten zu den Datenschutzschild-Grundsätzen der Benachrichtigung, Wahlfreiheit, Weiterübermittlung, Sicherheit, Datenintegrität, Zugänglichkeit und Durchsetzbarkeit bekennt. Weitere Informationen zum Datenschutzschild sowie eine Liste der derzeit für den Datenschutzschild zertifizierten Organisationen und die Bescheinigung von Lookout finden Sie hier: http://www.privacyshield.gov.

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.

Wenn Sie als EU-Ansässiger nicht damit zufrieden sind, wie wir auf Ihre Bedenken hinsichtlich 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, das Problem zu lösen.

In der EU ansässige Personen haben auch das Recht, ungelöste Beschwerden einer Schiedsstelle vorzulegen. 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. Jede Partei trägt ihre eigenen Anwaltsgebühren. Bitte beachten Sie, dass die Schiedsstelle(n) gemäß 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).

Neben den im obigen Abschnitt „Einstellungen einsehen und aktualisieren“ erläuterten Rechten haben internationale Anwender (darunter jene, deren Daten wir unter dem Datenschutzschild erfassen) in einigen Fällen bestimmte gesetzliche Rechte auf Einsichtnahme in bestimmte Daten, die wir über sie besitzen, und deren Löschung. Nehmen Sie über privacy@lookout.com mit uns Kontakt auf, wenn Sie zu dieser Nutzergruppe gehören und diese Rechte anwenden möchten.

Die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft trat, ist eine Initiative der Europäischen Union zum Schutz des Grundrechts von in der EU ansässigen Personen auf Privatsphäre. Demnach muss jede Organisation, die in irgendeiner Form mit personenbezogenen Daten von EU-Ansässigen in Kontakt kommt, diese Daten schützen. Um der Datenschutz-Grundverordnung (Verordnung [EU] 2016/679, „DSGVO“) nachzukommen, unternimmt Lookout jeden wirtschaftlich vertretbaren Aufwand, inklusive empfohlener technischer und organisatorischer Maßnahmen.

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

In der Europäischen Union und bestimmten anderen Rechtssystemen ansässige Personen haben gegebenenfalls bestimmte Rechte hinsichtlich (1) Anträgen auf Einsichtnahme oder Berichtigung oder Löschung der Daten, die wir über sie erfassen, (2) Anträgen auf Einschränkung der Verarbeitung ihrer Daten, (3) des Widerspruchs gegen die Verarbeitung ihrer Daten oder (4) Anträgen auf Übertragung bestimmter Daten (nur in ganz bestimmten Situationen). Wenn Sie diese oder andere Rechte ausüben möchten, wenden Sie sich bitte an Ihren Arbeitgeber (oder gegebenenfalls MDM-Anbieter). Darüber hinaus können Sie auch uns kontaktieren, die Kontaktdaten finden Sie nachstehend. Unter angemessenen Umständen können wir den Antrag an den Arbeitgeber weiterleiten und seinen Anweisungen zur Umsetzung Folge leisten. In Frankreich und bestimmten anderen Rechtssystemen ansässige Personen können auch vorgeben, wie wir ihre Daten nach

ihrem Tod aufbewahren, löschen oder weitergeben sollen. Gegebenenfalls können solche Personen auch jemanden nennen, der diese Rechte nach ihrem Tod ausübt.

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

Wenn Sie weitere Fragen haben, wenden Sie sich bitte an Ihren Arbeitgeber (oder gegebenenfalls MDM-Anbieter). Ihre Fragen können Sie auch an unseren Datenschutzbeauftragten unter privacy@lookout.com oder Lookout, Inc., Attn: Michael Musi, Data Privacy Officer, One Front Street, Suite 3100 San Francisco, CA 94111, USA, richten. Anschrift für EU-Ansässige: Lookout, Inc., Attn: G.J. Schenk, SVP International Sales, Florapark 3, 2012 HK Haarlem, Nederland.

Datum des Inkrafttretens: 25. Mai 2018