Datenschutzrichtlinie für Lookout Personal

Erstellt am: 15.11.2016
Überarbeitet am: 22.05.2018
Status: Genehmigt

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	22.09.2016	Erster Entwurf	Marcelo Guerra
2.0	26.09.2017	Überarbeitung	Joseph Leung
3.0	01.04.2018	Überarbeitet, um Produktänderungen und neue behördliche Vorschriften zu berücksichtigen. Details zum Revisionsverlauf verschoben an das Ende des Dokuments.	Kimberly Snow

Datum des Inkrafttretens: 25. Mai 2018

Bei diesem Dokument handelt es sich um unsere Datenschutzrichtlinie. Sie beschreibt, welche Informationen wir von Ihnen erfassen und wie wir sie nutzen. Lesen Sie neben der Datenschutzrichtlinie unbedingt auch die Lookout-Nutzungsbedingungen (unter www.lookout.com/legal/terms), denn beide regeln Ihre Nutzung der Lookout Personal-App. Unsere Datenschutzrichtlinie gilt für unsere Websites und mobilen Websites, z. B. www.lookout.com, unsere Lookout Personal-App sowie alle anderen Lookout-Dienste, die im Rahmen der Lookout Personal-App bereitgestellt werden (Definition siehe Nutzungsbedingungen).

Die Datenschutzrichtlinie für Lookout Mobile Endpoint Security für Unternehmen finden Sie in der Datenschutzerklärung von Lookout für Unternehmen.

Diese Datenschutzrichtlinie beschreibt die Erfassung und Nutzung personenbezogener Daten durch uns. Bei diesen Daten kann es sich beispielsweise um Ihren Namen, Ihre E-Mail-Adresse, Ihre Telefonnummer und/oder die eindeutige Kennung Ihres Mobilgeräts handeln. Unter „personenbezogenen Daten“ versteht die Datenschutz-Grundverordnung (Verordnung [EU] 2016/679, kurz: DSGVO) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Lookout behält sich das Recht vor, diese Datenschutzrichtlinie anzupassen, sollten Gesetzesänderungen, Änderungen an unseren Datenerfassungs- und Datennutzungspraktiken, Funktionsänderungen bei unseren Diensten oder technische und technologische Fortschritte dies erforderlich machen. Deshalb empfehlen wir Ihnen, dieses Dokument oder die Webseiten von Lookout.com regelmäßig zu lesen. Indem Sie mit der Nutzung unserer Dienste fortfahren, akzeptieren Sie solche Änderungen und verpflichten sich zur Einhaltung der überarbeiteten Richtlinie. Bei Fragen zu dieser Datenschutzrichtlinie erreichen Sie uns unter privacy@lookout.com. Sie können sie über den Anmeldebildschirm der Lookout-App, die Einstellungen in der Lookout Personal-App und auf unserer Firmenwebsite einsehen.

Das Produktangebot der Lookout Personal-App

Der Umfang der Lookout Personal-App variiert je nach gewählter Produktstufe, wobei die jeweils höhere Stufe mehr Lookout-Sicherheitsfunktionen bietet als die darunterliegende. Dadurch variiert auch der für die Dienstbereitstellung erforderliche Umfang an Informationen, die wir von Ihnen und Ihrem Gerät beziehen. Welche das sind und wie wir Sie nutzen, erfahren Sie in diesem Dokument. Informationen zu den Produktfunktionen der Lookout Personal-App für iOS- und Android-Geräte finden Sie unter https://www.lookout.com/products/personal/ios und unter https://www.lookout.com/products/personal/android.

1. Wir erfassen Ihre Daten, damit Sie unsere Lookout-Dienste nutzen können

Sofern nicht anders angegeben, speichern wir die Daten, die wir von Ihnen erfassen, und verknüpfen sie mit Ihrem Konto. Wir nehmen den Schutz Ihrer Privatsphäre sehr ernst und werden diese Informationen daher nur wie hierin beschrieben verwenden und offenlegen.

Einige unserer Produkte sind eigenständig und erfassen nur bestimmte oder gar keine Daten. Die Verfügbarkeit der Funktionen variiert nach Produkt und Land, daher gelten nicht alle Abschnitte dieser Datenschutzrichtlinie für solche Produkte.

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

Wir möchten Sie daran erinnern, dass wir Daten zu Anwendungen und Sicherheitsprüfungen erfassen, um Sie und Ihre Daten zu schützen und die Lookout-Dienste zu optimieren.

Darüber hinaus erfasst Lookout Daten zu Ihrem Gerät, darunter den Hersteller, das Modell, die Art und Version des Betriebssystems und die installierten Anwendungen. Diese Daten werden anonymisiert und mit anonymisierten Daten von anderen Kunden kombiniert, um Einblick in die regionalen Präferenzen für Geräte und Anwendungen zu gewinnen. Damit Ihre personenbezogenen Daten sicher sind, bleiben solche Informationen auch anonym. Durch die Kombination der Kundendaten auf sichere, die Vertraulichkeit wahrende Weise erhält Lookout besseren Einblick in aktuelle Sicherheitsbedrohungen und kann seine Sicherheitsfunktionen und -dienste verbessern. Gelegentlich veröffentlichen wir auch Berichte, die aus diesen Datenanalysen hervorgehen, um andere über mobile Bedrohungen und bestimmte App-Verhaltensweisen zu unterrichten.

2. Diese Daten erfasst Lookout für die Basisversion der Lookout Personal-App

a. Registrierungsdaten

Bei der Erstellung eines Kontos verlangen wir von Ihnen eine E-Mail-Adresse und ein Passwort.

b. Gerätedaten

Bei der Nutzung der Lookout-Dienste zeichnen unsere Server bestimmte Informationen über die Mobilgeräte der Anwender auf. Hierzu zählen Gerätekennungen (z. B. IMEI), Netzteilnehmerkennungen (z. B. IMSI), Gerätenamen, Mobiltelefonnummern, Gerätetypen und -hersteller, Betriebssysteme und ihre Versionen, Funknetzbetreiber, Netzwerktypen, Herkunftsländer, IP-Adressen (Internet Protocol) und Anforderungszeitpunkte. Außerdem erfassen wir Daten zu den Anwendungen auf Ihrem Gerät, um sie zu prüfen und Kopien der geprüften Anwendungsdateien herunterzuladen. Finden wir auf Ihrem Gerät eine von uns bisher nicht analysierte Anwendung, wird unter Umständen eine Kopie eines Teils oder der gesamten Anwendungsdateien auf Ihrem Gerät heruntergeladen. Ebenso erfassen wir unter Umständen Daten zum Verhalten von Anwendungen auf Ihrem Gerät (z. B. ob eine Anwendung SMS zu höheren als den Standardgebühren versendet und damit Ihre Mobilfunkrechnung erhöht) und Daten zu Netzwerkdiensten, mit denen Ihre Anwendungen kommunizieren. Letzteres dient dazu, unlauter agierende Anwendungen aufzuspüren (z. B. solche, die mit Servern kommunizieren, auf denen bekanntermaßen Phishing-Websites gehostet werden). Bei jeder Prüfung durch Lookout erfassen wir, welche Anwendungen dabei als potenziell unerwünscht eingestuft werden. Daraufhin empfiehlt Lookout Maßnahmen für den Umgang mit solchen Dateien (z. B. deinstallieren oder ignorieren).

Die oben beschriebenen Daten verwenden wir zur Bereitstellung unserer Dienste und, wenn nötig, technischer Unterstützung (Support). Außerdem erfassen wir Informationen über die Analyse mobiler Bedrohungen in aggregierter Form. Aggregierte Informationen sind anonymisiert, um die Identifizierung von Einzelpersonen zu verhindern.

Weitere Informationen zur Analyse mobiler Bedrohungen durch Lookout finden Sie unter https://www.lookout.com/de/why-lookout.

c. Standortdaten

Einige unserer Funktionen sind effektiver, wenn wir Ihr Mobilgerät orten können. Mit Ihrer Einwilligung, die Sie bei der Registrierung geben können, darf Lookout Standortdaten auf zweierlei Art erfassen. Zum einen können wir sie direkt von Ihrem Mobilgerät erhalten, zum anderen situationsbedingt über Funkmast- oder WLAN-Hotspot-Informationen. Unter Mitwirkung von externen Dienstleistern wandeln wir diese Informationen unter

Umständen in verwertbare Standortdaten um. Wenn Sie keine Standortdaten teilen möchten, schalten Sie die Standortdienste Ihres Mobilgeräts in dessen Einstellungen aus.

d. URLs

Für die Funktion „Sicheres Surfen“ übermitteln wir unter Umständen die URLs, die auf Ihrem Mobilgerät eingehen oder die Sie dort besuchen, an einen von Lookout oder Dritten bereitgestellten Dienst, der die Vertrauenswürdigkeit dieser URLs überprüft (d. h. ermittelt, ob über die URLs Phishing, Malware oder Exploits drohen). Wenn eine von Ihnen besuchte URL als unsicher gilt, verzeichnen wir dies in unserem Archiv. Unser Archiv an unsicheren URLs, die Sie aufrufen, nutzen wir, um (1) Sie darüber zu benachrichtigen, dass die URL, die Sie aufrufen wollten, unsicher ist (z. B. bei Ihrer nächsten Anmeldung auf der Lookout-Website oder per E-Mail), und um (2) unser Produkt zu verbessern und Analysen durchzuführen. Sollen die von Ihnen besuchten unsicheren URLs nicht protokolliert werden, können Sie „Sicheres Surfen“ deaktivieren – dies wird die Funktion der anderen Lookout-Funktionen nicht beeinträchtigen.

3. Die Funktionen der Lookout Personal-App

a. Sicherheit

Über mehrere Plattformen stellt Lookout Sicherheitsfunktionen bereit, die Ihr Gerät vor Cyberbedrohungen schützen sollen. Durch Ihre Nutzung der Lookout-App werden Informationen erfasst, die zur Unterstützung dieser Funktionen erforderlich sind. Mehr zu diesen Informationen erfahren Sie im Abschnitt „Gerätedaten“.

Die Lookout-Sicherheitsfunktionen, die sich je nach Plattform unterscheiden, schützen auf unterschiedliche Weise, beispielsweise durch Prüfungen auf schädliche Apps und Dateien sowie die Erkennung veralteter Betriebssysteme. Weitere Informationen zur vorausschauenden Sicherheit von Lookout finden Sie auf www.lookout.com. In regelmäßigen Abständen kann es zur automatischen Prüfung Ihres Geräts kommen, deren Zweck es ist, Details zu dessen Anwendungen und Betriebssystem sowie zum Gerät selbst zu erfassen. Lookout trägt die Ergebnisse der Prüfungen, die unsere Dienste durchführen, und den aktuellen Sicherheitsstatus des Geräts zusammen. Darüber hinaus werden die Bedrohungsdefinitionen regelmäßig aktualisiert. Diese Maßnahmen dienen dem Schutz Ihres mobilen Endpunkts, weil die Lookout-App dadurch Bedrohungen auf Ihrem Mobilgerät erkennen und beheben kann. Diese Funktion lässt sich in den Einstellungen der Lookout-App ein- und ausschalten.

b. Geräteverlust

Die Diebstahlschutzfunktionen von Lookout erstrecken sich auch auf Geräte, die bereits abhanden gekommen sind, z. B. die Remote-Funktion „Lokalisierung und Gerätealarm“, die Sie über Ihr Personal-Konto unter

lookout.com nutzen können. Und sollte Ihrem verloren gegangenen Handy der Akku ausgehen, können Sie per „Signal Flare“ die letzte bekannte Position abrufen. Diese Funktion erfasst Standortdaten und sendet sie an Lookout, sobald der Akkustand bedenklich niedrig ist. Erhalten wir die Akkuwarnung, speichern wir den Standort des Geräts auf lookout.com. Diese Funktion lässt sich in den Einstellungen der Lookout-App ein- und ausschalten.

Sind die Geräteverlustfunktionen aktiviert, sendet Ihr Browser externen Landkartenanbietern (z. B. Google Maps) Standortdaten, um den Standort in Ihrem Personal-Konto auf lookout.com auf einer Karte anzuzeigen. Nach der Aktivierung dieser Funktion orten wir Ihr Gerät einige Minuten lang, um den Standort präzise zu bestimmen. Diese Informationen verbleiben in Ihrem Kontoverlauf, woraus Sie sie über die Kontoeinstellungen jederzeit löschen können. Sobald Sie diese Informationen löschen oder Ihr Konto deaktivieren, anonymisiert Lookout diese Daten, sodass sie nicht mehr mit Ihren personenbezogenen Daten verknüpft sind.

c. Backup (Kontakte)

Mit Lookout Backup können Anwender ihre Kontakte sichern. Die dabei entstehenden Daten erreichen die Lookout-Cloudserver über ein verschlüsseltes Protokoll. In Ihrem Konto auf Lookout.com können Sie diese Daten einsehen oder löschen. Diese Funktion lässt sich in den Einstellungen der Lookout-App ein- und ausschalten.

d. Unterstützung mehrerer Geräte

Mehrere Geräte lassen sich mit einem Hauptkonto verknüpfen, welches das Gerät des Hauptkontoinhabers sowie bestimmte Funktionen der anderen verknüpften Geräte kontrolliert. Die Inhaber solcher Hauptkonten können so über einige Funktionen der zusätzlichen Geräte bestimmen, zum Beispiel, ob ein Nutzer eines solchen Mehrgerätekontos Backup-Daten eines verknüpften Geräts suchen oder einsehen kann.

4. Daten, die Lookout für die Premiumdienste der Personal-App erfasst

a. Datenerfassung beim Upgrade auf den Premiumdienst

Wie auch in der Basisversion der Personal-App erfasst Lookout Registrierungs-, Geräte- und Standortdaten (wenn nötig). Darüber hinaus erfasst Lookout aber auch Zahlungsdaten, um Ihnen Premiumfunktionen bereitzustellen.

b. Zahlungsdaten

Wenn Lookout Ihnen die Dienste „Premium“ oder „Premium Plus“ direkt verkauft, beauftragen wir einen

externen Anbieter für die Zahlungsabwicklung damit, Ihre Kreditkartendaten wie Nummer, Ablaufdatum, Prüfziffer und sonstige erforderliche Zahlungsinformationen zu erfassen. Anhand dieser Daten wird unser externer Lieferant Ihnen die Nutzung der Dienste in Rechnung stellen. Lookout verfügt über Informationen zu Ihrem „Premium“- und/oder „Premium Plus“-Konto, darunter die Zahlungssumme und die Zahlungsmethode. Ihre Kreditkarten- oder Bankkontodaten haben wir allerdings nicht, diese verbleiben beim externen Zahlungsabwickler.

Wenn Sie die Lookout-App in einem App-Store oder über den Datentarif Ihres Betreibers erwerben, regeln der jeweilige App-Store bzw. Betreiber den Umgang mit Ihren Zahlungsdaten. Die Zahlungen gehen nicht bei Lookout ein, außerdem können vielfältige Methoden auf die Abwicklung Ihrer Zahlung angewendet werden. Unsere Partner sichern vertraglich zu, dass Sie die erwartete Leistung der Lookout-App erhalten. Damit wir Ihnen unsere Dienste zur Verfügung stellen können, erhält Lookout vom App-Store eine Bestätigung Ihres Kaufs. Netzbetreiber können Ihre Telefonnummer, Teilnehmerkennung, SKU und sonstige nichtfinanzielle Informationen weitergeben. Weder der App-Store noch der Betreiber geben jedoch Ihre Kreditkarten- oder Abrechnungsdaten weiter. Weitere Informationen finden Sie in den Zahlungsabwicklungs-Richtlinien und -Verfahrensweisen des jeweiligen App-Stores oder Betreibers.

c. Datenerfassung bei Diebstahlwarnung

Bei aktivierter Diebstahlwarnung wird ein Foto aufgenommen. Zusammen mit Standortdaten (GPS-Position) wird es kurz auf unseren Servern gespeichert, damit wir Ihnen eine E-Mail mit dem Bild und einer Karte mit dem Standort Ihres Geräts zusenden können. Danach wird das Bild vom Server gelöscht. Die E-Mail geht an die mit Ihrem Konto verknüpfte Adresse, sorgen Sie also bitte dafür, dass diese E-Mail-Adresse in Ihren Kontoeinstellungen stets aktuell ist. Um unsere Produkte zu analysieren, zu optimieren und zu reparieren verwenden wir Daten über die Aktivitäten der Diebstahlwarnfunktion auf Ihrem Gerät.

d. Sicheres Surfen

Die Funktion zum sicheren Surfen erkennt unsichere URLs und warnt Sie davor, damit Sie sie nicht unbeabsichtigt laden. „Sicheres Surfen“ ist verfügbar, wenn Sie der App den Betrieb eines lokalen VPNs gestattet haben. Über dieses VPN prüft die Funktion URLs, die Ihr Gerät über Browser und andere Apps aufruft. Die besuchten URLs werden anonymisiert und zur Lookout-Cloud gesendet, wo die Sicherheitsprüfungen stattfinden. Diese URLs sind dann auch die einzigen Daten zu Ihrer Browseraktivität, die zu Lookout gelangen; wir erfassen hierbei keine Suchverläufe oder sonstige personenbezogene Daten.

5. Die Premiumfunktionen von Lookout

Neben den vorstehend beschriebenen Funktionen erhalten „Premium“-Kunden von Lookout auch Zugang zu neuen und verbesserten Funktionen.

a. Geräteverlust

Abonnenten des Premiumdienstes von Lookout profitieren von einer umfangreicheren Geräteverlustfunktion. So können sie das Gerät über das Personal-Konto bei lookout.com aus der Ferne sperren und die Gerätedaten löschen lassen.

b. Diebstahlwarnung

Die Diebstahlwarnung ist eine Premiumfunktion beim Diebstahlschutz und ermöglicht die Ortung abhanden gekommener Mobilgeräte. Ist sie aktiviert, erhalten Sie in bestimmten Situationen (z. B. bei aktiviertem Flugmodus) eine E-Mail mit der Position Ihres Geräts. Geht ein Android-Gerät verloren oder wird es gestohlen, beinhaltet diese E-Mail ein Foto des möglichen Diebs, aufgenommen von der Kamera des Geräts, und Standortmerkmale, anhand derer Sie die Position des Geräts (und denjenigen, der es nun hat) genauer eingrenzen können.

Den Gerätestandort sehen Sie in Ihrem Konto auf Lookout.com. Für diese Funktion sind die Standortdaten Ihres Geräts sowie die E-Mail-Adresse und Telefonnummer, die Sie Lookout über das Gerät übermittelt haben, erforderlich, damit sie Ihnen beim Auffinden des Handys nützt.

c. Backup (Anrufliste und Fotos)

Abonnenten des Premiumdienstes profitieren von Backups der Anrufliste und Fotos. In Ihrem Personal-Konto auf Lookout.com haben Sie Einsicht in die Fotos, die Sie, genau wie die Backup-Daten, jederzeit aus dem Konto löschen können.

d. Sicheres Surfen

Die Funktion zum sicheren Surfen erkennt unsichere URLs und warnt Sie davor, damit Sie sie nicht unbeabsichtigt laden. „Sicheres Surfen“ ist verfügbar, wenn Sie der App den Betrieb eines lokalen VPNs gestattet haben. Über dieses VPN prüft die Funktion URLs, die Ihr Gerät über Browser und andere Apps aufruft. Die besuchten URLs werden anonymisiert und zur Lookout-Cloud gesendet, wo die Sicherheitsprüfungen stattfinden. Diese URLs sind dann auch die einzigen Daten zu Ihrer Browseraktivität, die zu Lookout gelangen; weder erfassen wir hierbei Suchverläufe noch sonstige personenbezogene Daten.

e. Sicheres WLAN

Die Funktion für ein sicheres WLAN untersucht Ihre WLAN-Verbindung auf ungewöhnliche Aktivitäten, die auf Sicherheitslücken oder Angriffe im Netzwerk hindeuten können. Im Ernstfall erhalten Sie dann eine Benachrichtigung. „Sicheres WLAN“ trägt dazu bei, Ihre personenbezogenen Daten im Mobilgerät vor Hackerangriffen zu schützen.

f. Bericht über Datensicherheitsverletzungen (nur in englischer Sprache)

Lookout benachrichtigt Sie über relevante Datenpannen und gibt Ihnen im selben Bericht nützliche Tipps, wie Sie sich selbst besser schützen können. Sie können einstellen, ob Sie diese „Breach Reports“ zu bestimmten Unternehmen oder Branchen wünschen, und erhalten Handlungsempfehlungen zum Daten- und Identitätsschutz.

g. Funktionen deaktivieren

In den Lookout-Einstellungen können Sie Funktionen nach Wunsch deaktivieren. Bei Problemen und Fragen stehen wir Ihnen unter support@lookout.com gern zur Verfügung.

6. Datenerfassung durch Lookout Premium Plus (nur USA)

Welche Daten wir erfassen, hängt davon ab, für welche „Premium Plus“-Identitätsschutzprodukte Sie sich registrieren. Wir benötigen sie, um Ihre Identität zu bestätigen, Ihnen die gewünschten Identitätsschutzdienste bereitzustellen und diese mit den vereinbarten Gebühren in Rechnung zu stellen. Um Ihnen diese Dienste zur Verfügung zu stellen, müssen wir Ihre Daten an Dritte weitergeben (z. B. Stellen zur Bestätigung von Identitätsnachweisen bzw. Zahlungen, Kreditauskunfteien, Strafverfolgungsbehörden usw.). Außerdem können wir die Daten unseren externen Dienstleistern übergeben, die uns bei der Bereitstellung von Identitätsschutzdiensten unterstützen, oder ihnen erlauben, bestimmte Daten von Ihnen direkt zu erfassen. Diesen Dienstleistern ist es wiederum gestattet, Ihre Daten Dritten zu geben, um Ihnen die gewünschten Dienste bereitzustellen. Im Rahmen dieser Identitätsschutzdienste können wir und/oder unsere Dienstleister Ihre Identität überwachen oder Sie benachrichtigen sowie Daten und Berichte über Sie (oder andere, die in Ihrem Namen registriert sind) einholen. Bei den fraglichen Daten kann es sich um bisherige Anschriften sowie Namen, Aliasse und andere Berichte handeln. Wir verlangen von unseren Dienstleistern, die Nutzung der über Sie erfassten Daten auf den Zweck der Dienstbereitstellung über die „Premium Plus“-Version der Lookout-App zu beschränken. Wenn Sie sich auf ein „Premium Plus“-Abonnement mit Versicherung gegen Identitätsdiebstahl hochstufen lassen, verwenden wir im Fall einer Identitätsmanipulation Ihre Daten, um Unterstützung und den anwendbaren Versicherungsschutz zu leisten.

Wenn Sie sich für „Premium Plus“ registrieren, fragt die Lookout-App möglicherweise Ihre Kontaktdaten (z. B. Name, Anschrift, Telefonnummer und E-Mail-Adresse), persönliche Informationen (z. B. Nummer der Fahrerlaubnis, Sozialversicherungsnummer, Passnummer oder andere identifizierende Nummern), Finanzdaten (z. B. Kontonummer, Debit- und Kreditkartennummern), Krankenversichertennummer und andere personenbezogene Daten zu Ihnen (oder anderen, die in Ihrem Namen für den Dienst registriert sind) ab. Weitere Informationen sowie Updates finden Sie im Produktbereich von Lookout.com.

7. Die Funktionen von Lookout Premium Plus (nur USA)

„Premium Plus“-Anwender profitieren neben den Basisfunktionen (Geräteverlust, Sicherheit und Backup) und Premiumfunktionen (Diebstahlwarnung, Sicheres WLAN, Breach Reports, Foto-Backup) auch von Identitätsschutz, der Überwachung, Versicherung und Wiederherstellung umfasst.

1. Identitätsüberwachung

Mit einem Upgrade zu Lookout Premium Plus erhalten Sie Zugriff auf Dienste zum Schutz Ihrer Identität und personenbezogenen Daten.

a. Cyber-Überwachung

Diese Funktion sucht im Internet nach persönlichen Informationen über Sie und benachrichtigt Sie, inklusive Handlungsempfehlungen, sobald sie im öffentlichen Raum fündig wird.

b. Social Media Watch

Diese Funktion überwacht das Schutzniveau Ihrer personenbezogenen Daten in sozialen Netzwerken und benachrichtigt Sie bei unangemessenen Beiträgen.

c. SSN Watch

Diese Funktion benachrichtigt Sie, wenn neue Namen oder Anschriften mit Ihrer Sozialversicherungsnummer verknüpft sind.

2. Versicherung und Wiederherstellung

Lookout übernimmt die mühevolle Wiederstellung gekaperter Identitäten.

a. Versicherung gegen Identitätsdiebstahl

Lookout Premium Plus bietet eine Versicherung, die Anwaltskosten, entgangenes Gehalt und andere Ausgaben

im Rahmen der Wiederherstellung einer gekaperten Identität abdeckt.

b. Hilfe bei der Wiederherstellung

Die Lookout-Experten für die Identitätswiederherstellung stehen Ihnen rund um die Uhr zur Verfügung.

c. Hilfe bei Brieftaschenklau

Falls Ihre Brieftasche verloren geht oder gestohlen wird, unterstützt Lookout Sie beim Sperren und Ersetzen von Geldkarten, Identitätsnachweisen und Sonstigem.

8. Für KDDI-Kunden: Kundendienst durch Mobilfunkanbieter

Wenn Ihr Mobiltelefon oder Tablet verloren geht oder gestohlen wird, können Sie Ihren Mobilfunkanbieter mit dessen Suche und Sicherstellung beauftragen, sofern Ihr Mobilfunkanbieter an unserem „Mobile Operator Customer Care“-Programm beteiligt ist.

Für einen funktionierenden Kundendienst benötigt Lookout Informationen zu Ihnen und Ihrem Gerät, deshalb erfasst die Kundendienst-Webanwendung (Customer Care Web Application) Ihre Telefonnummer, sofern verfügbar, und Details zum Gerätetyp und Betriebssystem. Dies stellt sicher, dass die Kundendienstmitarbeiter die Remote-Funktionen Ihres Geräts kennen und verwalten können.

Lookout stellt den Kundendienstmitarbeitern Ihre Informationen zu Verfügung, damit diese Sie im erwarteten Umfang unterstützen können.

Durch die Kundendienst-Webanwendung können Mobilfunkanbieter und deren Kundendienstmitarbeiter auf Ihren Wunsch hin die Remote-Funktionen Ihres Geräts verwenden, z. B.:

- Geräteortung
- Gerätesperre
- Datenlöschung auf dem Gerät
- Aktivierung eines lauten Signals (Gerätealarm)
- Senden von Nachrichten an das Gerät

Nur auf Ihren Wunsch und mit Ihrer vorherigen Zustimmung sind die Kundendienstmitarbeiter zur Ausführung solcher Funktionen befugt.

Zum Schutz der Privatsphäre von Anwendern benachrichtigt Sie Lookout jedes Mal, wenn ein Kundendienstmitarbeiter eine der obigen Funktionen ausführt, per E-Mail unter der für Sie hinterlegten

Adresse. Kundendienstmitarbeiter können Anwenderdaten, die durch die Lookout-App gesichert werden, weder einsehen noch kontrollieren.

9. Datenanalysen: Verwendung der über Ihren mobilen Endpunkt erfassten Daten

Anhand der Ergebnisse unserer Datenanalysen können wir Ihnen relevante Inhalte senden sowie neue Funktionen, Produkte und/oder Dienste vorschlagen, die Ihr Lookout-Erlebnis verbessern können. Die Informationen, die wir in der Analysesoftware speichern, verknüpfen wir nicht mit personenbezogenen Daten, die Sie in der App übermitteln. Aggregierte Informationen sind zudem anonymisiert, um die Identifizierung natürlicher Personen zu verhindern.

Die Daten, die wir von Ihnen erhalten und die wir über Ihren mobilen Endpunkt erfassen, nutzen wir nicht nur, um die Lookout-Dienste bereitzustellen, sondern in letzterem Fall auch, um Datenanalysen durchzuführen. Solche Analysen liefern wichtige Informationen zur Verbesserung der Funktionen und Bedienerfreundlichkeit unserer Produkte. Analysiert werden unter anderem die Häufigkeit Ihrer Nutzung der Lookout-App auf dem Mobilgerät, die Ereignisse in der Lookout-App auf dem Mobilgerät und der Zeitpunkt, an dem die Lookout-App auf das Mobilgerät heruntergeladen wurde. Des Weiteren aggregieren wir diese Informationen und nutzen Sie für Analysen zu bekannten und neuen Bedrohungen für Mobilgeräte.

10. Ihre Nutzung der (mobilen) Lookout-Website und unsere Datenerfassung

Wenn Sie die Lookout-Website über Ihren stationären Computer oder Ihr Mobilgerät aufrufen, kann Lookout freiwillig von Ihnen zur Verfügung gestellte Daten nutzen, um das Anwendererlebnis zu verbessern. Zudem kann Lookout mit Analysendiensten im Hintergrund das Nutzungsverhalten hinsichtlich unserer Website und E-Mails messen. Dies dient dem Zweck, unsere Produkte und Dienste zu verbessern und Ihnen relevantere Inhalte zu präsentieren. Für die Analyse unserer (mobilen) Website können wir Bilddateien einbetten, die nicht angezeigt werden, aber mit eindeutigen Kennungen auf unserer Website ausgestattet sind. Darüber hinaus können Cookies oder andere lokale Speichertechnologien sowie Zählpixel und ähnliche Tracking-Technologien für die Analyse verwendet werden.

a. Inhalte und Promoaktionen

Während Ihres Besuchs auf unseren Websites bitten wir Sie eventuell um Ihre E-Mail-Adresse und andere Kontaktdaten, damit wir Ihnen Zugang zu Lookout-Inhalten wie Whitepapers, Videos oder anderem Recherchematerial geben können. Darüber hinaus bieten wir Ihnen gelegentlich die Teilnahme an Umfragen, Wettbewerben, Promoaktionen oder Verlosungen an oder bitten Sie um Feedback zu Ihren Erfahrungen mit den Diensten und Produkten von Lookout. Anhand Ihrer Kontaktdaten senden wir Ihnen zusätzliche

Informationen zu den Produkten und Diensten von Lookout oder unseren Geschäftspartnern. Indem Sie in einer unserer E-Mails auf den Link zum Abbestellen von Mitteilungen (weitere Infos nachstehend) klicken, entscheiden Sie sich gegen den Erhalt solcher Marketingbotschaften.

b. Social-Media-Funktionen

Unsere Website verfügt über Social-Media-Funktionen („Funktionen“) wie die „Gefällt mir“-Schaltfläche oder interaktive Miniprogramme. Wenn Sie diese Funktionen nutzen, erfassen sie Ihre IP-Adresse sowie die von Ihnen besuchte Seite auf unserer Website und sie setzen Cookies, um die ordnungsgemäße Ausführung der Funktionen sicherzustellen. Die Funktionen können von Dritten oder direkt auf unserer Website gehostet werden. Ihre Interaktionen mit Funktionen von Dritten unterliegen der Datenschutzrichtlinie des jeweiligen Anbieters, nicht aber der von Lookout.

11. Cookie-Richtlinie für die Lookout-Website

1. Cookie-Typen

Wie viele Online-Dienste verwenden wir Cookies und andere Tools, um Daten über Sie und Ihre Nutzung unserer Produkte und Dienste zu erfassen und zu analysieren. Solche Technologien erlauben es uns, Ihnen relevante Inhalte zu den Produkten und Diensten von Lookout bereitzustellen. Cookies sind kleine Datendateien, die wir auf Ihrem Computer oder Mobilgerät ablegen. Weitere Details finden Sie auf aboutcookies.org.

2. So nutzen wir Cookies

Mithilfe unserer „Sitzungs“-Cookies bleiben Sie während des Gebrauchs unserer Dienste angemeldet. Dies verschafft uns einen Einblick in Ihre Art der Dienstnutzung; diese Daten und Daten zum Webdatenverkehr über unsere Dienste bündeln und überwachen wir als Ganzes. Sitzungs-Cookies werden gelöscht, wenn Sie sich abmelden und den Browser schließen. Darüber hinaus nutzen wir „permanente“ Cookies, durch die wir Sie wiedererkennen, wenn Sie unsere Dienste mehrmals nutzen. Sofern Sie diese Cookies nicht löschen, verbleiben sie länger auf Ihrem Computer als Sitzungs-Cookies. Schließlich verwenden wir auch noch „Analyse“-Cookies. Mit ihnen zählen wir Besucher, erkennen sie wieder und verfolgen, wie sie in den Diensten navigieren und diese verwenden. Dadurch können wir die Funktionalität unserer Website verbessern, beispielsweise, indem wir beliebte Informationen leichter auffindbar machen. Zudem können wir andere gebräuchliche Technologien wie Zählpixel und lokale Speichertechnologien nutzen, um Daten zu Ihrer Nutzung der Produkte und Dienste zu erfassen, zu analysieren und zu aggregieren.

3. Cookies von Dritten

Wir möchten Sie detailliert darüber informieren, welche Drittpartei-Cookies wir auf unserer Website und in unseren Diensten nutzen, daher finden Sie nachstehend eine Liste der Drittpartei-Cookies bei uns, die personenbezogene Daten zu Ihren Online-Aktivitäten über einen gewissen Zeitraum sowie Websites und Online-Dienste von Dritten hinweg erfassen können. Im Zuge der Weiterentwicklung und Verbesserung unserer Dienste arbeiten wir unter Umständen mit weiteren Dritten zusammen; diese Liste wird dann dementsprechend aktualisiert. Nachstehend finden Sie auch Links zu den Cookie-Richtlinien der Drittparteien.

- Google Analytics: Anhand dieser Cookies erfahren wir, wie Sie unsere Website und App nutzen, sodass wir anhand dieser Daten das Nutzererlebnis verbessern können. Bitte lesen Sie hierzu die Datenschutzerklärung von Google. Wenn Sie die Datenübermittlung durch Google Analytics nicht wünschen, bietet Google ein Browser-Add-on zur Deaktivierung von Google Analytics.
- Google AdWords: Mithilfe dieser Cookies können unsere Partner Anzeigen auf Basis Ihrer früheren Besuche auf unseren Websites sowie im Rahmen des Remarketing bereitstellen. Diese Cookie-Technologie und andere Tracking-Technologien kann Google nutzen, um unsere Anzeigen im Internet bereitzustellen. Wenn Sie diese Art der Cookie-Verwendung ablehnen, können Sie dies in den Anzeigeneinstellungen von Google festlegen.
- Marketo: Mithilfe dieser Cookies können wir Ihre Besuche unserer Websites nachverfolgen und eine überzeugende Marketingstrategie entwickeln. Zudem ermöglichen Marketo-Cookies es uns, Ihnen relevante Informationen zukommen zu lassen, da sie Einblick in Ihren Umgang mit unseren E-Mails bieten: So übermitteln Marketo-Cookies, ob Sie unsere E-Mails öffnen und welche Links Sie darin anklicken. Hier steht Ihnen die Datenschutzerklärung von Marketo zur Verfügung.
- Social-Media-Funktionen: Unsere Website verfügt über Social-Media-Funktionen wie Empfehlungsschaltflächen oder interaktive Miniprogramme. Wenn Sie diese Funktionen nutzen, erfassen sie Ihre IP-Adresse sowie die von Ihnen besuchte Seite auf unserer Website und sie setzen Cookies, um die ordnungsgemäße Ausführung der Funktionen sicherzustellen. Die Funktionen können von Dritten oder direkt auf unserer Website gehostet werden. Ihre Interaktionen mit solchen Funktionen unterliegen der Datenschutzrichtlinie des jeweiligen Anbieters, nicht aber der von Lookout.
- Mixpanel, Braze und mParticle: Mithilfe dieser Cookies können wir Daten zur Nutzung unserer App analysieren und aggregieren. Bitte lesen Sie hierzu die Datenschutzerklärungen von MixPanel, Braze und mParticle.

12. Die rechtliche Grundlage für die Nutzung Ihrer Daten

Für die in dieser Datenschutzrichtlinie erläuterte Nutzung Ihrer Daten durch uns gilt folgende Rechtsgrundlage: (a) Die Nutzung Ihrer personenbezogenen Daten ist notwendig, damit wir unsere Pflichten aus Verträgen mit Ihnen erfüllen können (z. B. zur 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 anderer (z. B. zur Gewährleistung der Sicherheit der Lookout-Dienste, für den Betrieb und die Vermarktung der Lookout-Dienste, zur Schaffung einer sicheren Umgebung für unser Personal und andere Personen, zum Ausführen und Erhalten von Zahlungen, zur Betrugsprävention und zu unserer genaueren Kenntnis der Kunden, die unsere Lookout-Dienste nutzen). In einigen Fällen geschieht die Verarbeitung personenbezogener Daten, um geltende Gesetze einzuhalten.

In bestimmten Fällen (z. B. bei einer Reihe von Marketingaktivitäten) verarbeiten wir Ihre Daten nur mit Ihrer Einwilligung.

Außer zu den vorstehenden Zwecken verwenden wir Ihre Daten auch folgendermaßen:

a. Bereitstellung, Verbesserung und Vermarktung unserer Dienste

Anhand Ihrer Daten können wir Ihnen besseren Service bieten, unsere Produkte und Dienste verbessern, unsere Dienste bewerben und neue Dienste entwickeln. Hier einige Beispiele:

- Durch die Teilnahme an Umfragen oder mit einer E-Mail an den Lookout-Support senden Sie uns Daten, die wir speichern dürfen, um Ihnen Support zu leisten und unsere Dienste zu verbessern.
- Sofern verfügbar, nutzt Lookout Daten über Client-Geräte, um Sie über notwendige Updates Ihres Betriebssystems zu informieren.
- Eventuell senden wir Ihnen SMS, um mit dem Mobiltelefon zu kommunizieren.
- Eventuell nutzen wir Ihre E-Mail-Adresse oder Mobiltelefonnummer, um Ihnen Hinweise zu den Themen Datenschutz oder Sicherheit sowie Benachrichtigungen zu wesentlichen Änderungen der Lookout-Dienste zu senden.
- Eventuell nutzen wir Ihre E-Mail-Adresse oder Mobiltelefonnummer, um Produkte und Sonderaktionen von Lookout oder unseren Geschäftspartnern anzukündigen oder Ihre Teilnahme an Sonderveranstaltungen, Umfragen, Wettbewerben und Verlosungen zu verwalten.

- Eventuell nutzen wir Ihre Daten zu Marktforschungszwecken und zur Ausführung gemeinsamer Promoaktionen mit Unternehmen, deren Produkte einen Mehrwert für Lookout-Produkte oder -Dienste darstellen können (z. B. Mobilfunkanbieter).

b. Gesetzeskonforme Offenlegung Ihrer Daten

Wie andere Unternehmen auch dürfen wir Ihre Daten gemäß gesetzlichen Bestimmungen offenlegen, z. B. aus diesen Gründen: (i) zur Einhaltung eines Gesetzes, einer Vorschrift oder eines Rechtsprozesses (inkl. der Einhaltung von Bestimmungen zur nationalen Sicherheit oder Strafverfolgung); (ii) zum Schutz oder zur Absicherung von natürlichen und juristischen Personen sowie Einrichtungen; (iii) zum Umgang mit möglichen Verstößen gegen unsere Datenschutzrichtlinie oder Nutzungsbedingungen; (iv) zur Ermittlung bei Betrug, Sicherheitsverstößen oder technischen Problemen; oder (v) zum Schutz der Rechte oder des Eigentums von Lookout oder Dritten, unserer Mitarbeiter, Anwender und der Öffentlichkeit.

Uns ist es ein wichtiges Anliegen, Sie zu informieren, wenn wir von Gesetzes wegen verpflichtet sind, Ihre Daten weiterzugeben. Deshalb benachrichtigen wir Sie per E-Mail an die in Ihrem Konto hinterlegte Adresse, ehe wir Ihre Daten im Rahmen eines Antrags der Strafverfolgungsbehörden (z. B. eine Vorladung oder eine gerichtliche Anordnung) weitergeben. Von dieser Regel weichen wir ab, wenn (a) uns diese Handlung verboten ist oder (b) ein Notfall vorliegt, bei dem die Benachrichtigung mit dem Risiko von Verletzungen oder Tod einhergeht oder möglicherweise Minderjährige zu Schaden kommen könnten. Darüber hinaus ist nichts in dieser Datenschutzrichtlinie darauf ausgelegt, Ihre gesetzlichen Verteidigungen oder Widersprüche zu beschränken, die Sie gegen Offenlegungsanträge seitens Dritter (auch der Regierung) vorbringen können.

c. Weitergabe Ihrer Daten zur Bereitstellung oder Verbesserung unserer Dienste

Wir teilen Ihre Daten mit anderen Gesellschaften unserer Unternehmensgruppe oder mit Dritten, um unsere Dienste bereitzustellen oder zu verbessern. Hier einige Beispiele:

- Wir können Ihre Daten an externe Anbieter von in unsere Software integrierten Produkten und Diensten weitergeben, damit diese Ihre Anforderungen an die Produkte oder Dienste erfüllen (z. B. Erfassung Ihres Standorts, Senden von SMS oder Bereitstellung von Identitätsschutzdiensten), unsere Produkte und Dienste unterstützen oder Daten zum Zweck der Performancemessung und Produktverbesserung analysieren können.
- Wir können Ihre Daten an Mobilfunkanbieter weitergeben, die an unserem „Mobile Operator Customer Care“-Programm teilnehmen, damit diese Sie auf Ihren Wunsch direkt über unsere Kundendienst-Webanwendung (Customer Care Web Application) mit Lookout-Geräteverlustfunktionen wie Ortung, Sperre, Datenlöschung oder Gerätealarm unterstützen können.

- Wir können Ihre Daten zum Zweck der Buchhaltung, Betriebsprüfung, Abrechnungsabstimmung und für Inkassoaktivitäten weitergeben.
- Wir können Ihre Daten an unsere verbundenen Unternehmen, Händler oder andere externe Dienstanbieter weitergeben, die mit Lookout zusammenarbeiten (z. B. Mobilfunk- und MDM-Anbieter), um die ordnungsgemäße Bereitstellung Ihrer Käufe und zugehörigen Supportdienste sicherzustellen, geschäftsrelevante Funktionen auszuführen und Sie über Produkte und Dienste zu informieren.

13. Nutzung Ihrer Daten in Sicherheitsberichten

Zur Datenanalyse anonymisieren, bündeln und verdichten wir Daten, zu denen auch Daten von Ihnen gehören können. Mit Ihrer Einwilligung dürfen wir Ihre Daten offenlegen und Ihre personenbezogenen Daten an Dritte weitergeben.

14. Ihre Optionen

a. Einstellungen einsehen und aktualisieren

Über Ihr Lookout-Konto auf unserer Website und/oder die Seite „Einstellungen“ in der Lookout-App können Sie festlegen – und diese Einstellungen ändern –, welche Daten mit uns geteilt werden, z. B., indem Sie das Backup bestimmter Datentypen deaktivieren. Zum Schutz Ihrer Privatsphäre und zu Ihrer Sicherheit müssen Sie Ihren Nutzernamen und das Passwort angeben, um Ihre Identität vor dem Zugriff auf das Konto zu bestätigen oder bevor Sie Änderungen vornehmen. Wenn Sie Ihre personenbezogenen Daten berichtigen oder falsche Angaben löschen lassen oder die von uns erfassten personenbezogenen Daten über Sie einsehen möchten, wenden Sie sich bitte an privacy@lookout.com. Wir werden innerhalb von 30 Tagen auf Ihre Anfrage reagieren. In einigen Fällen kann es jedoch sein, dass Lookout Ihnen keinen Einblick verschaffen oder nicht alle personenbezogenen Daten löschen kann, die wir über Sie haben.

b. Widerspruch per E-Mail

Sie können Werbebotschaften von Lookout abbestellen, indem Sie auf den entsprechenden Link klicken, der in jeder E-Mail angegeben ist. Solche Stornierungen werden in der Regel sofort bearbeitet, bitte lassen Sie uns trotzdem zehn (10) Geschäftstage Zeit, um Sie aus der Liste auszutragen. Auch nachdem Sie dem Erhalt von Werbebotschaften widersprochen haben, senden wir Ihnen transaktions- und produktrelevante Mitteilungen zu den Lookout-Diensten. In den Kontoeinstellungen können Sie einigen dieser Benachrichtigungen widersprechen.

c. Personalisierte Anzeigen

Bestimmten personalisierten Anzeigen von Mitgliedern der Network Advertising Initiative oder Unternehmen, die sich den Selbstregulierungsprinzipien der Digital Advertising Alliance zu gezielter Online-Werbung verpflichten, können Sie widersprechen. Um Werbung von Programmteilnehmern direkt abzulehnen, besuchen Sie die Widerspruchsseite der Network Advertising Initiative für Verbraucher oder die der Digital Advertising Alliance. Diese Tools und die Optionen, die Werbetreibende und andere über diese Tools bieten, unterliegen weder der Kontrolle von Lookout noch werden sie von Lookout betrieben.

d. Standort

Wenn Sie Standortdaten in Ihrem Konto-Dashboard auf Lookout.com löschen, sind sie nicht mehr mit Ihrem Konto verknüpft und werden in unseren Anwendungs-Produktionssystemen anonymisiert.

15. Datenaufbewahrungsrichtlinie

Wir verpflichten uns dazu, personenbezogene Daten nur so lange aufzubewahren, wie dies angemessenerweise nötig ist, um Ihnen unsere Produkte und Dienste bereitzustellen, oder wie es anderweitig zur Einhaltung gesetzlicher Compliance-Vorschriften erforderlich ist. Bei Inaktivität Ihres Kontos oder wenn anderweitig durch unsere Nutzungsbedingungen vorgeschrieben können wir Ihre Daten löschen.

16. Beiträge im Blog oder Community-Forum sind öffentlich

Bitte beachten Sie: Wenn Sie Kommentare in unserem Blog oder anderen öffentlichen Foren hinterlassen, können andere Blognutzer sie lesen, erfassen oder verwenden, z. B. zum Senden unerwünschter Nachrichten. Wir sind nicht verantwortlich für Informationen, die Sie in diesen Blogbeiträgen übermitteln, oder Inhalte, die Sie aufgrund der mitgeteilten Informationen erhalten.

17. Unser Sicherheitsversprechen

Lookout ist ein auf Sicherheit spezialisiertes Unternehmen, deshalb verpflichten wir uns zum Schutz Ihrer Daten. Mithilfe eines wirtschaftlich vertretbaren Maßes an physischen, administrativen und technischen Schutzmaßnahmen sorgen wir für den passenden technischen und organisatorischen Rahmen. So schützen wir Ihr Konto und Ihre Daten mit einer Kombination aus Firewalls, Authentifizierungstechnologie, Sicherheits-Hardware und so weiter. Sensible Informationen (z. B. Kreditkartendaten oder Standortdaten), die Sie auf unserer Website, in der Lookout-App oder in unseren Bestellformularen eingeben, übertragen wir SSL-verschlüsselt (Secure Socket Layer). Außerdem schließen wir mit Penetrationstests durch Dritte potenzielle Schwachstellen unserer Systeme. Lookout ergreift alle angemessenen Maßnahmen zur Umsetzung von

Kontrollmechanismen und zum Schutz vor komplexen technologischen und anderen kriminellen Bedrohungen sowie vor nachlässigem Verhalten der Mitarbeiter.

Keine internetbasierte Übertragungsmethode und keine Methode der elektronischen Speicherung ist hundertprozentig sicher, daher können wir die Sicherheit der Informationen, Daten oder Inhalte nicht zusichern, die Lookout in Ihrem Auftrag für den Betrieb der Lookout-Dienste erhält oder die Sie Lookout übermitteln. Sie erhalten und senden sämtliche Daten aus freien Stücken und auf eigenes Risiko. Wir können nicht garantieren, dass diese Daten nicht durch die Überwindung unserer physischen, technischen und administrativen Schutzmaßnahmen eingesehen, offengelegt, geändert oder vernichtet werden.

Erfährt Lookout von einer Datenpanne, versuchen wir, Sie auf elektronischem Wege zu benachrichtigen, damit Sie angemessene Schutzmaßnahmen durchführen können. Darüber hinaus wird Lookout auch Mitteilungen über Datenpannen in die Lookout-Dienste einstellen. Je nach Ihrem Wohnort haben Sie eventuell das gesetzliche Recht, schriftlich über eine Datenpanne informiert zu werden.

18. Ihre Verantwortung, Ihre E-Mail-Adresse und das Passwort aktuell und vertraulich zu halten

Sie sind dafür verantwortlich, Ihr Passwort nicht offenzulegen. Wir empfehlen, ein starkes Passwort anzulegen, dass Sie nur für diesen Dienst nutzen. Wenn Sie den Verdacht haben, Ihr Passwort sei gestohlen worden, ändern Sie es bitte unverzüglich über die Lookout-Website oder bitten Sie unter support@lookout.com um Unterstützung. Sie sind dafür verantwortlich, die mit Ihrem Konto verknüpfte E-Mail-Adresse aktuell zu halten. Anhand dieser E-Mail-Adresse kontaktieren wir Sie zu Dienst-Updates, Änderungen an unseren Richtlinien und Kontoaktivitäten wie Anträge auf Dateneinsicht oder Versuche, Ihr Gerät zu orten. Lookout ist nicht verantwortlich, wenn Dritte aufgrund einer vom Nutzer falsch angegebenen E-Mail-Adresse personenbezogene Daten erhalten.

19. Hinweis für Anwender in Kalifornien

a. Nachverfolgungssperre „Do Not Track“

Die Nachverfolgungssperre „Do Not Track“ können Anwender in ihren Webbrowsern einrichten. Ist das „Do Not Track“-Signal aktiviert, sendet der Browser Websites den Auftrag, den Anwender nicht nachzuverfolgen. Weitere Informationen zu dieser Nachverfolgungssperre finden Sie auf www.allaboutdnt.org. Derzeit reagieren wir nicht auf „Do Not Track“-Browsereinstellungen oder -signale. Einige unserer externen Dienstanbieter nutzen möglicherweise auch Standardtechnologien wie Cookies und Zählpixel, um Ihre Internetaktivitäten zu

erfassen. Wie und in welchem Umfang Sie dieses websiteübergreifende Tracking durch Dritte deaktivieren können, ist oben im Abschnitt „Ihre Optionen“ beschrieben.

20. Internationale Besucher, der Datenschutzschild und die DSGVO

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, 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 privacy@lookout.com oder per Post an die Adresse im Abschnitt „Kontaktaufnahme bei Fragen oder Bedenken“. 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.

Unser Aufwand umfasst:

Identifizierung personenbezogener Daten: Jeder Lookout-Dienst erfordert ein anderes Maß an personenbezogenen Daten, die erfasst, verwendet, gespeichert und beseitigt werden müssen. Dieses Maß und die diversen Quellen personenbezogener Daten müssen für jeden Dienst festgelegt und dokumentiert werden, damit Lookout überblickt, welche personenbezogenen Daten erfasst werden, und die Daten angemessen verwalten und schützen kann.

Ermöglichen der Einsichtnahme und Transparenz: Lookout bietet Einsicht in und Zugang zu personenbezogenen Daten, indem wir zeitnah und gemäß den DSGVO-Bestimmungen auf Kundenanfragen reagieren. Anfragen richten Sie bitte an support@lookout.com. Zum Einsehen und Aktualisieren von personenbezogenen Daten nutzen Sie bitte Ihr persönliches Lookout-Webportal.

Sicherstellen der Datenintegrität und -sicherheit: Lookout gewährleistet Datenintegrität durch die strikte

Kontrolle des Zugriffs auf Kundendaten. Darüber hinaus verschlüsselt Lookout personenbezogene Daten bei der Übertragung und Speicherung.

21. Anwender unter 16 Jahren

Lookout hat einen internationalen Kundenstamm für seine Dienste. Um also sowohl US-amerikanische als auch EU-Gesetze (Chapter 91 – Children's Online Privacy Protection Act und DSGVO-Artikel 8 – Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) einzuhalten, erfasst oder speichert Lookout nicht wissentlich personenbezogene Daten zu Kindern unter 16 Jahren, es sei denn, sie fallen unter Mehrgerätekonten von Eltern, die der Datenerfassung und -speicherung gemäß den Lookout-Nutzungsbedingungen zustimmen. Wenn Sie vermuten, dass ein Kind den Dienst ohne Einwilligung der Eltern nutzt, wenden Sie sich bitte an privacy@lookout.com.

22. Wir sind nicht verantwortlich für Inhalte auf den Websites Dritter

Unsere Website enthält Links zu anderen Websites. Wenn Sie auf einen dieser Links klicken, wechseln Sie von der Lookout-Website zu einer anderen Website. Lookout haftet nicht für den Missbrauch von Daten durch Verantwortliche für Websites, auf die wir möglicherweise verweisen. Wir empfehlen dringend, die Datenschutzerklärungen dieser verlinkten Websites zu lesen, da diese von unserer abweichen können. Außerdem kann es vorkommen, dass Sie einem unserer Partner Daten direkt zur Verfügung stellen, wenn Sie auf dessen Angebot eingehen. Auch hier empfehlen wir dringend, die Datenschutzerklärungen unserer Partner zu lesen, da wir nicht für die Datenschutzpraktiken unserer Partner oder verlinkten Websites verantwortlich sind.

23. Kontrollwechsel

Im Falle einer Insolvenz, Fusion, Übernahme, Neuorganisation oder Veräußerung von Vermögensgegenständen werden Ihre Daten eventuell als Teil der Transaktion verkauft oder übertragen.

24. Hinweise auf der Website bei Änderungen an der Richtlinie

Änderungen an unseren Produkten und Diensten sowie Änderungen auf Basis von Gesetzen, denen Lookout und Sie unterliegen, werden sich eventuell auf diese Richtlinie auswirken und zu deren Abänderung führen. Sollten wir die Richtlinie wesentlich ändern, benachrichtigen wir Sie hierzu in unserer Anwendung, hier auf der Website, per E-Mail oder in einem Hinweis auf der Lookout-Startseite. Wenn Sie unsere Dienste dann weiternutzen, stimmen Sie der neuen Datenschutzrichtlinie zu und verpflichten sich zu ihrer Einhaltung. Wenn

Sie nicht möchten, dass Ihre Daten der überarbeiteten Datenschutzrichtlinie unterliegen, müssen Sie Ihr Konto schließen.

25. Kontaktaufnahme bei Fragen oder Bedenken

Bei Fragen oder Anmerkungen zu dieser Richtlinie erreichen Sie 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. In der EU ansässige Personen können sich auch an Hr. G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Niederlande, wenden.