Lookout, Inc.
Anwendung „Personal“
Datenschutzerklärung

Datum des Inkrafttretens:
01.01.2020
Erstellt am: 15.11.2016
Überarbeitet am: 01.01.2020

1. EINLEITUNG 3

2. VON UNS ERFASSTE DATEN 3

A. DATENKATEGORIEN. LOOKOUT ODER DIE PARTNER VON LOOKOUT KÖNNEN IM RAHMEN DER NUTZUNG DER PERSONAL-APP DIE FOLGENDEN DATENKATEGORIEN VON IHNEN ERFASSEN: 3

B. DIESE DATEN ERFASST LOOKOUT FÜR DIE BASIS-VERSION DER LOOKOUT PERSONAL-APP 4

C. DIESE DATEN ERFASST LOOKOUT FÜR DIE PREMIUM-VERSION DER LOOKOUT PERSONAL-APP 4

D. DIESE DATEN ERFASST LOOKOUT FÜR DIE PREMIUM PLUS-VERSION DER LOOKOUT PERSONAL-APP 5

E. DIESE DATEN ERFASST LOOKOUT VON DRITTEN 5

LOOKOUT EMPFÄNGT ANALYSEDATEN VON DRITTEN, WIE VORSTEHEND BESCHRIEBEN. 5

3. SO VERWENDEN WIR IHRE DATEN. 5

4. SO GEBEN WIR IHRE DATEN WEITER 6

5. IHRE WAHLMÖGLICHKEITEN 8

A. EINSTELLUNGEN EINSEHEN UND AKTUALISIEREN 8

B. ABLEHNUNG DES ERHALTS VON E-MAILS 8

6. DATENSPEICHERUNG 8

7. SICHERHEIT 8

A. VERANTWORTLICHKEITEN VON LOOKOUT 8

B. IHRE VERANTWORTLICHKEITEN. 8

8. BENUTZER UNTER 16 JAHREN 9

9. INTERNATIONALE ÜBERMITTLUNGEN VON DATEN 9

10. ZUSÄTZLICHE BEDINGUNGEN FÜR EINWOHNER DES EUROPÄISCHEN WIRTSCHAFTSRAUMS („EWR“) 9

A. RECHTLICHE GRUNDLAGE FÜR DIE VERARBEITUNG. 9

B. IHRE RECHTE 10

11. KONTAKTAUFNAHME BEI FRAGEN ODER BEDENKEN 11

1. Einleitung

Bei diesem Dokument handelt es sich um unsere Datenschutzerklärung für die Anwendung „Personal“ (die „Erklärung“). Sie beschreibt, welche personenbezogenen Daten von uns erfasst werden, wenn Sie die Anwendung „Lookout Personal“ (die „Personal-App“) verwenden, und wie wir diese Daten nutzen. Bitte lesen Sie neben der Erklärung unbedingt auch die Nutzungsbedingungen von Lookout (unter www.lookout.com/legal/terms), denn beide regeln Ihre Nutzung der Lookout Personal-App. Alle von Lookout auf andere Weise als durch Ihre Nutzung der Personal-App erhobenen personenbezogenen Daten unterliegen einer anderen Datenschutzerklärung.

Änderungen an unseren Produkten und Diensten sowie Änderungen auf Basis von Gesetzen, denen Lookout und Sie unterliegen, werden sich eventuell auf diese Erklärung auswirken und zu deren Abänderung führen. Wenn wir wesentliche Änderungen an dieser Erklärung vornehmen, werden wir Sie darüber in Kenntnis setzen. Wenn Sie nicht möchten, dass Ihre Daten der überarbeiteten Erklärung unterliegen, müssen Sie Ihr Konto schließen.

Sie können die Erklärung über den Anmeldebildschirm der Lookout-App, die Einstellungen in der Lookout Personal-App und auf unserer Firmenwebsite einsehen.

2. Von uns erfasste Daten.

Der Umfang der 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 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.

a. Datenkategorien. Lookout oder die Partner von Lookout können im Rahmen der Nutzung der Personal-App die folgenden Datenkategorien von Ihnen erfassen:

i. ***Registrierungsdaten,*** einschließlich einer E-Mail-Adresse und eines Passworts.

ii. ***Gerätedaten,*** wie beispielsweise Gerätekennung (z. B. Mobiltelefonnummer, Gerätetyp und -hersteller, Typ und Version des Betriebssystems, Mobilfunkanbieter/Netzbetreiber, Netzwerktyp, Herkunftsland, SSID des WLAN-Netzwerks, Internetprotokoll-Adresse („IP-Adresse“) sowie Datum und Uhrzeit Ihrer Anfragen.

iii. ***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 von Teilen der Anwendung oder der gesamten Anwendung auf Ihrem Gerät erfassen können, wenn wir auf eine nicht zuvor von uns analysierte Anwendung stoßen. Diese Daten sind pseudonymisiert und werden in aggregierter Form aufbewahrt, um die Identifizierung einer natürlichen Person durch andere Kunden zu verhindern. 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.

iv. ***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. Dies kann sich jedoch auf die Funktionen von Lookout auswirken.

v. ***Daten für Diebstahlwarnungen,*** einschließlich Standortdaten und einem Bild, das bei der Aktivierung der Diebstahlwarnung aufgenommen wird.

vi. ***Zahlungsdaten,*** einschließlich Ihrer Kreditkartennummer, des Ablaufdatums, des Sicherheitscodes und anderer anwendbarer Abrechnungsdaten – diese Daten können direkt von den Partnern von Lookout erfasst werden, wenn Sie die Version „Premium“ oder „Premium Plus“ der Anwendung erwerben.

vii. ***Daten über Webinhalte,*** einschließlich URLs und Domains in Bezug auf böswillige Inhalte und Inhalte, die einer zusätzlichen Analyse bedürfen, um festzustellen, ob diese URLs unsicher sind (z. B. ob die URLs Phishing-Angriffe oder Malware umfassen). Lookout erfasst keinen Browserverlauf.

viii. ***Daten zum Schutz vor Identitätsdiebstahl***, die Sie beim Kauf von Lookout „Premium Plus“ angeben können, einschließlich persönlicher Daten (z. B. Führerscheinnummer, Sozialversicherungsnummer, Passnummer oder andere Identifikationsnummern), Finanzdaten (z. B. Kontonummer, Debit- und Kreditkartennummern), Krankenversicherungsnummer und andere personenbezogene Daten zu Ihrer Person (oder anderen Personen, die in Ihrem Namen für den Dienst registriert sind), einschließlich Name und Titel – diese Daten können direkt vom Lookout-Partner CSIdentity (jetzt Teil von Experian) erfasst werden.

ix. ***Analysedaten,*** einschließlich Tools von Drittanbietern wie Mixpanel, Braze und mParticle, um uns bei der Analyse und Aggregierung von Daten bezüglich Ihrer Nutzung unserer Dienste zu unterstützen. Bitte lesen Sie hierzu die Datenschutzerklärungen von MixPanel, Braze, und mParticle.

Da die Produkteigenschaften je nach Stufe variieren, kann Lookout wie nachstehend beschrieben und abhängig von der von Ihnen gewählten Stufe verschiedene Arten von Daten erfassen.

b. Diese Daten erfasst Lookout für die Basis-Version der Lookout Personal-App

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

ii. ***Gerätedaten.*** Bei der Nutzung der Lookout-Dienste zeichnen unsere Server wie im vorstehenden Abschnitt 2(a)(ii) beschrieben bestimmte Daten über Ihr Mobilgerät auf.

iii. ***Anwendungsdaten.*** Bei der Nutzung der Lookout-Dienste erfassen wir Daten zur Anwendung und laden eine Kopie eines Teils oder der gesamten Anwendungsdateien auf Ihrem Gerät heruntergeladen, wenn wir auf Ihrem Gerät eine von uns bisher nicht wie im vorstehenden Abschnitt 2(a)(iii) beschrieben analysierte Anwendung finden. Lookout erfasst keine Daten, die Nutzer in diese Anwendungen 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.

iv. ***Standortdaten.*** Sofern die Funktion zur Ortung eines verloren gegangenes Gerät aktiviert ist, verwendet Lookout die entsprechenden Standortdaten, um Ihnen dabei zu helfen, Ihr Telefon in der Nähe seines letzten bekannten Standorts zu lokalisieren, sollten Sie es verlieren und der Akku erschöpft sein. Zusätzlich erfasst diese Funktion, wenn Sie „Signal Flare“ aktiviert haben, Standortdaten und übermittelt diese an Lookout, wenn Ihr Akku zur Neige geht.

c. Diese Daten erfasst Lookout für die Premium-Version der Lookout Personal-App

Lookout erfasst für diese Version dieselben Daten, wie sie für die Basisversion der Personal-App erhoben werden. Zusätzlich zu diesen Daten erfassen die Partner von Lookout jedoch auch Zahlungsdaten direkt von Ihnen, um Ihnen den Zugriff auf Premium-Funktionen, Daten über Webinhalte für die Nutzung der Funktion zum sicheren Surfen und Daten zu Diebstahlwarnungen für die Meldung von Diebstählen wie nachstehend beschrieben zu ermöglichen.

i. ***Zahlungsdaten.*** Wenn Sie ein Abonnement für die Lookout-Dienste „Premium“ oder „Premium Plus“ direkt bei uns erwerben, beauftragen wir einen externen Zahlungsdienstleister mit der Erfassung Ihrer Zahlungsdaten. 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 Zahlung geht nicht an Lookout. Außerdem können vielfältige Methoden auf die Abwicklung Ihrer Zahlung angewendet werden. 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.

ii. ***Daten über Webinhalte.*** Lookout verwendet Daten über Webinhalte, damit Ihnen die Funktion zum sicheren Surfen zur Verfügung gestellt werden kann. 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.

iii. ***Daten zur Diebstahlwarnung.*** Wenn die Diebstahlwarnung aktiviert ist, 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.

d. Diese Daten erfasst Lookout für die Premium Plus-Version der Lookout Personal-App

Lookout erfasst für diese Version dieselben Daten, wie sie für die Premium-Version der Personal-App erhoben werden. Zusätzlich zu diesen Daten erfassen die Partner von Lookout jedoch auch Daten zum Schutz vor Identitätsdiebstahl von Ihnen.

i. ***Daten zum Schutz vor Identitätsdiebstahl.*** Wenn Sie die Funktion zum Schutz vor Identitätsdiebstahl verwenden, können Sie die vorstehend genannten Daten zum Schutz vor Identitätsdiebstahl eingeben, um sich für bestimmte Dienste zur Überwachung des Identitätsschutzes anzumelden Diese Leistungen werden von unserem Partner CSIdentity (jetzt Teil von Experian) erbracht. Die von CSIdentity zu Ihrer Person erfassten und gespeicherten Daten richten sich nach den Informationen, die Sie in die Personal-App eingeben. Um Ihnen diese Dienstleistungen anbieten zu können, muss CSIdentity Ihre Daten zum Schutz vor Identitätsdiebstahl möglicherweise an Dritte (z. B. Stellen zur Bestätigung von Identitätsnachweisen bzw. Zahlungen, Kreditauskunfteien, Strafverfolgungsbehörden usw.) weitergeben.

e. Diese Daten erfasst Lookout von Dritten

Lookout empfängt Analysedaten von Dritten, wie vorstehend beschrieben.

3. So verwenden wir Ihre Daten.

Sofern nicht anders angegeben, speichern wir die Daten, die wir von Ihnen erfassen, und verknüpfen diese mit Ihrem Konto. Bitte beachten Sie, dass wir bestimmte Arten von Daten benötigen, damit wir Ihnen die Dienste zur Verfügung stellen können. Wenn Sie uns diese Informationen nicht zur Verfügung stellen oder uns auffordern, sie zu löschen, haben Sie eventuell keinen Zugriff mehr auf die Dienste. Wir nehmen den Schutz Ihrer Privatsphäre sehr ernst und werden diese Daten nur für die in dieser Erklärung beschriebenen geschäftlichen und kommerziellen Zwecke verwenden und weitergeben. Wie wir Ihre Daten verwenden, hängt von der Art der Daten ab und wird im Folgenden beschrieben:

a. Anwendungsdaten. Wir verwenden diese Daten zur Bereitstellung unserer Dienste, indem wir die Dateien der Anwendungen zur Feststellung des böswilligen Verhaltens der Anwendungen scannen. Darüber hinaus pseudonymisieren wir Daten und aggregieren die Informationen, um die Beliebtheit von Anwendungen nach Regionen zu ermitteln und unsere Analyse hinsichtlich mobiler Bedrohungen durchzuführen. Diese Daten zur Analyse mobiler Bedrohungen verbleiben pseudonymisiert, um den Datenschutz zu gewährleisten. Durch die Kombination von Kundendaten auf sichere, die Vertraulichkeit wahrende Weise erhält Lookout einen besseren Einblick in die aktuellen Sicherheitsbedrohungen und kann die Lookout-Dienste weiter verbessern.

b. **Gerätedaten**. Es kann in regelmäßigen Abständen zu automatischen Prüfungen Ihres Geräts kommen, deren Zweck es ist, Details zu dessen Anwendungen und Betriebssystem sowie zum Gerät selbst zu erfassen. Lookout trägt die Ergebnisse der von unseren Diensten durchgeführten Prüfungen sowie den aktuellen Sicherheitsstatus des Geräts zusammen. Darüber hinaus werden die Bedrohungsdefinitionen regelmäßig aktualisiert. Diese Maßnahmen dienen dem Schutz Ihres mobilen Endpunkts, weil die Personal-App dadurch Bedrohungen auf Ihrem Mobilgerät erkennen und beheben kann. Sofern verfügbar, nutzt Lookout Daten über Client-Geräte, um Sie über notwendige Updates Ihres Betriebssystems zu informieren. 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 letztendlich auch zur Durchführung von Datenanalysen. Derartige Analysen liefern wichtige Informationen zur Verbesserung der Funktionen und Bedienerfreundlichkeit unserer Produkte. Analysiert werden unter anderem die Häufigkeit Ihrer Nutzung der Lookout-Anwendung auf dem Mobilgerät, die Ereignisse in der Lookout-Anwendung auf dem Mobilgerät und der Zeitpunkt, an dem die Lookout-Anwendung auf das Mobilgerät heruntergeladen wurde. Des Weiteren aggregieren wir diese Informationen und nutzen Sie für Analysen zu bekannten und neuen Bedrohungen für Mobilgeräte.
c. **Daten zum Schutz vor Identitätsdiebstahl**. CSIdentity verwendet diese Daten, um Ihre Identität zu bestätigen und Ihnen die angeforderten Dienstleistungen zum Schutz Ihrer Identität zur Verfügung zu stellen. Wenn Sie sich auf ein „Premium Plus“-Abonnement mit Versicherung gegen Identitätsdiebstahl hochstufen lassen, verwenden unsere Partner im Fall einer Identitätsmanipulation Ihre Daten, um Unterstützung und den anwendbaren Versicherungsschutz zu leisten.
d. **Standortdaten.** Die Funktion zur Ortung eines verloren gegangenen Geräts von Lookout ermöglicht es Ihnen, Ihr Gerät über Ihr persönliches Konto unter lookout.com per Fernzugriff zu lokalisieren und akustisch zu aktivieren. Dabei verwendet Lookout die entsprechenden Standortdaten, um Ihnen dabei zu helfen, Ihr Telefon in der Nähe seines letzten bekannten Standorts zu lokalisieren, sollten Sie es verlieren und der Akku erschöpft sein. 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 unter lookout.com. Diese Funktion kann über die Einstellungen der Personal-App aktiviert oder deaktiviert werden.
e. **Registrierungsdaten.** Wir verwenden unter Umständen Ihre E-Mail-Adresse, um Ihnen Informationen über Produktankündigungen und Sonderangebote von Lookout oder unseren Geschäftspartnern zukommen zu lassen. Wenn Sie eine E-Mail an den Lookout-Support senden, speichern wir diese Daten unter Umständen, um Ihnen unsere Unterstützung anbieten und unsere Dienstleistungen verbessern zu können. Wir nutzen Ihre E-Mail-Adresse möglicherweise dazu, um Ihnen über das Gerät Informationen bezüglich der Dienste zukommen zu lassen, einschließlich der Versendung von Datenschutz- oder Sicherheitshinweisen und der Benachrichtigung über wichtige Änderungen der Lookout-Dienste.
f. **Daten zur Diebstahlwarnung**. Wir verwenden diese Informationen, um die Dienstleistungen zur Warnung vor Diebstahl erbringen zu können.
g. **Daten über Webinhalte.** Die Funktion zum sicheren Surfen erkennt unsichere URLs und warnt Sie davor, damit Sie diese nicht unbeabsichtigt aufrufen. Die besuchten URLs werden pseudonymisiert und an Lookout übermittelt, um Sicherheitsprüfungen durchzuführen. Wir verwenden die Aufzeichnung über die von Ihnen aufgerufenen unsicheren URLs, um Sie darauf hinzuweisen, dass die URL, die Sie zu erreichen versuchten, nicht sicher ist.

4. So geben wir Ihre Daten weiter

Dieser Abschnitt beschreibt, wie Lookout Ihre Daten weitergeben und offenlegen kann.

a. **Drittanbieter und Partner**. 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, unsere Produkte und Dienste unterstützen oder Daten zum Zweck der Performancemessung und Produktverbesserung analysieren können. Hier einige Beispiele:

i. Wenn Sie den Dienst zum Schutz vor Identitätsdiebstahl nutzen, werden Ihre Daten von unserem Partner CSIdentity (jetzt Teil von Experian) erfasst, damit Ihnen dieser Dienst zur Verfügung gestellt werden kann. CSIdentity kann wiederum Ihre Daten an Dritte weitergeben, wie z. B. an Stellen zur Bestätigung von Identitätsnachweisen, an Verbraucherschutzverbände, Kreditauskunfteien, Unternehmen zur Validierung von Zahlungen, Strafverfolgungsbehörden usw., um Ihnen die gewünschten Dienstleistungen anbieten zu können. CSIdentity kann Ihnen außerdem Überwachungs- und Warnmeldungen zur Verfügung stellen und Informationen und Berichte über Sie (oder andere Personen, die in Ihrem Namen registriert sind) einholen, um die Dienste zum Identitätsschutz bereitzustellen, darunter bisherige Anschriften sowie Namen, Aliasse und andere Berichte. Wir verlangen von CSIdentity und seinen Dienstleistern, die Nutzung der über Sie erfassten Daten auf den Zweck der Dienstbereitstellung über die „Premium Plus“-Version der Lookout-App zu beschränken.

ii. Wir können Ihre Daten an unsere Vertriebspartner oder andere Mobilfunkbetreiber weitergeben, um die ordnungsgemäße Bereitstellung Ihrer Käufe und der zugehörigen Supportdienste sicherzustellen und geschäftsrelevante Funktionen auszuführen.

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

b. **Externe Zahlungsdienstleister**. Wir können es Dienstleistern ermöglichen, Daten direkt von Ihnen zu erfassen, damit diese Aufgaben im Bereich der Buchhaltung, der Rechnungsprüfung, des Rechnungsabgleichs und des Inkassos durchführen.

c. **Einhaltung von Gesetzen**. Wir können 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 Datenschutzerklärung; (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 aufgrund von Gesetzen dazu 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 Datenschutzerklärung darauf ausgelegt, Ihre gesetzlichen Verteidigungen oder Widersprüche zu beschränken, die Sie gegen Offenlegungsanträge seitens Dritter (auch der Regierung) vorbringen können.

d. **Bei einer Änderung des Geschäftsbereichs von Lookout**. Wir können Ihre Daten auch einem tatsächlichen oder potenziellen Käufer (und seinen Vertretern und Beratern) im Zusammenhang mit einem tatsächlichen oder geplanten Kauf, einer Fusion oder der Übernahme eines Teils unseres Unternehmens offenlegen, vorausgesetzt, dass wir den Käufer darüber informieren, dass er Ihre Daten nur für die in dieser Datenschutzerklärung angegebenen Zwecke verwenden darf.

e. **Pseudonymisierte und aggregierte Daten**. Zur Datenanalyse pseudonymisieren, bündeln und aggregieren wir Daten, zu denen auch Daten von Ihnen gehören können. Gelegentlich veröffentlichen wir auch Berichte, die aus diesen Datenanalysen hervorgehen, um andere über mobile Bedrohungen und bestimmte App-Verhaltensweisen zu unterrichten.

f. **Mit Ihrer Einwilligung**. Wir können Ihre Daten auch an Dritte weitergeben, wenn uns Ihre Einwilligung dazu vorliegt.

5. Ihre Wahlmöglichkeiten

a. Einstellungen einsehen und aktualisieren

Sie können die Einstellungen Ihres Lookout-Kontos über die Seite „Einstellungen“ in unserer mobilen Anwendung oder durch Einloggen auf unserer Website unter https://my.lookout.com/user/login aktualisieren, um bestimmte Einstellungen zu ändern, die sich auf die an uns weitergeleiteten Daten auswirken. Zum Schutz Ihrer Privatsphäre und zu Ihrer Sicherheit müssen Sie Ihren Benutzernamen und Ihr Passwort angeben, um Ihre Identität vor dem Zugriff auf Ihr Konto oder vor Änderungen daran zu verifizieren.

b. Ablehnung des Erhalts von E-Mails

Sie können den Erhalt von Werbemitteilungen von Lookout abbestellen, indem Sie auf den entsprechenden Link klicken, der in jeder E-Mail angegeben ist. Zwar werden derartige Anfragen zur Abmeldung in der Regel sofort bearbeitet, wir bitten Sie jedoch um eine Bearbeitungszeit von zehn (10) Werktagen, um Sie aus der entsprechenden Liste auszutragen. Auch nachdem Sie dem Erhalt von Werbemitteilungen widersprochen haben, senden wir Ihnen transaktions- und produktrelevante Mitteilungen zu den Lookout-Diensten zu. In den Konto-Einstellungen können Sie dem Erhalt einiger dieser Mitteilungen widersprechen.

6. Datenspeicherung

Lookout speichert Ihre Daten, einschließlich Ihrer personenbezogenen Daten (gemäß der Begriffsbestimmung der DSGVO), nur so lange, wie es vernünftigerweise notwendig ist, um Ihnen unsere Produkte und Dienste zur Verfügung zu stellen, oder wie es anderweitig für die Einhaltung von Gesetzen erforderlich ist.

7. Sicherheit

a. Verantwortlichkeiten von Lookout

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, der dem Risiko der Verarbeitung Ihrer Daten angemessen ist. So schützen wir Ihr Konto und Ihre Daten beispielsweise mit einer Kombination aus Firewalls, Authentifizierungstechnologien, Sicherheits-Hardware und so weiter. Wenn Sie sensible Daten (wie z.B. Standortdaten) in der Lookout-App eingeben, verschlüsseln wir diese Daten während der Übertragung und der Speicherung mit der SSL-Technologie (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.

Wenn Lookout von einem Sicherheitsverstoß Kenntnis erlangt, von dem Sie betroffen sein könnten, werden wir versuchen, Sie auf elektronischem Wege darüber zu benachrichtigen, damit Sie geeignete Schutzmaßnahmen ergreifen können. Darüber hinaus wird Lookout auch Mitteilungen über Sicherheitsverstoß in den Lookout-Diensten veröffentlichen. In Abhängigkeit von Ihrem Wohnort haben Sie eventuell das gesetzliche Recht, schriftlich über einen Sicherheitsverstoß informiert zu werden.

b. Ihre Verantwortlichkeiten.

Sie sind dafür verantwortlich, Ihr Passwort stets geheim zu halten. 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 für Daten, die aufgrund der Angabe einer falschen E-Mail-Adresse durch den Benutzer an einen Dritten übermittelt werden.

8. Benutzer 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.

9. Internationale Übermittlungen von 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 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 vom US-Handelsministerium herausgegebenen Rahmenwerk des EU-US-Datenschutzschilds und Schweiz-US-Datenschutzschilds zertifiziert, das die Erfassung, Verwendung und Aufbewahrung personenbezogener Daten aus der Europäischen Union, dem Vereinigten Königreich und der Schweiz regelt. 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 eine Liste der derzeit für den Datenschutzschild zertifizierten Organisationen 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.

Wir unterliegen bezüglich der gemäß den Rahmenwerken zum Datenschutzschild erhaltenen oder übermittelten personenbezogenen Daten den gesetzlichen Durchsetzungsbefugnissen des US-amerikanischen Handelsministeriums. In bestimmten Situationen kann es erforderlich sein, dass wir auf rechtmäßige Anfragen von öffentlichen Behörden hin personenbezogene Daten offenlegen müssen, unter anderem um die Anforderungen an die nationale Sicherheit oder die Strafverfolgung zu erfüllen.

10. Zusätzliche Bedingungen für Einwohner des Europäischen Wirtschaftsraums („EWR“)

a. Rechtliche Grundlage für die Verarbeitung.

Wenn Sie ein im EWR ansässiger Benutzer sind, ist Lookout der für die Verarbeitung Ihrer personenbezogenen Daten Verantwortliche (entsprechend der Begriffsbestimmung in der Datenschutz-Grundverordnung („DSGVO“)). Die rechtliche Grundlage für die Erfassung und Verwendung Ihrer personenbezogenen Daten, wie in dieser Datenschutzerklärung dargelegt, hängt von den betreffenden personenbezogenen Daten und vom spezifischen Zweck ab, für den wir sie erfassen. Normalerweise werden wir Ihre personenbezogenen Daten jedoch nur dann erfassen, wenn Folgendes der Fall ist: (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) die Nutzung Ihrer personenbezogenen Daten ist für unsere berechtigten Interessen oder die berechtigten Interessen

anderer notwendig (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); oder (c) wir haben Ihre Einwilligung zur Nutzung Ihrer personenbezogenen Daten eingeholt (z. B. für einige unserer Marketingaktivitäten). In einigen Fällen erfolgt die Verarbeitung von personenbezogenen Daten, um geltende Gesetze einzuhalten.

b. Ihre Rechte.

Gemäß der DSGVO genießen die im EWR ansässigen Personen die nachstehend aufgeführten Rechte. Wenn Sie eines dieser Rechte ausüben möchten, kontaktieren Sie uns bitte unter privacy@lookout.com. 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.

i. **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.

ii. **Recht auf Berichtigung.** Sie haben das Recht, die Berichtigung aller fehlerhaften oder unvollständigen personenbezogenen Daten zu verlangen, die wir zu Ihrer Person gespeichert haben.

iii. **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. Zusätzlich zu den Rechten, die im obigen Abschnitt „Einstellungen einsehen und aktualisieren“ genannt werden, können Sie sich mit Ihrer Anfrage an privacy@lookout.com wenden.

iv. **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.

v. **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.

vi. **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.

vii. **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 Lookout sich auf die Einwilligung als Grundlage für die rechtmäßige Verarbeitung von „besonderen Kategorien personenbezogener Daten“, wie in der DSGVO definiert sind, beruft, wäre eine „explizite Einwilligung“ erforderlich.

Wenn Sie 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. Sie haben außerdem 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 des US-amerikanischen Handelsministeriums.

11. Kontaktaufnahme bei Fragen oder Bedenken

Bei Fragen oder Anmerkungen zu dieser Erklärung erreichen Sie unseren Datenschutzbeauftragten unter privacy@lookout.com oder per Post unter Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 28 State Street, 19th Floor, Boston, MA 02109, USA. Im EWR ansässige Personen können sich auch an Hr. G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Niederlande, wenden.