Lookout, Inc.

App Lookout for Work

Informativa sulla privacy

Data di efficacia: 01/04/2023

Data origine: 24/10/2016

Informativa sulla privacy dell'app Lookout for Work

È ferma convinzione di Lookout, Inc. ("Lookout", l'"Azienda") che la privacy degli utenti sia tanto importante quanto la loro sicurezza, per cui desidera fornire loro la massima trasparenza in merito ai dati che vengono raccolti per la salvaguardia del dispositivo utilizzato e la sicurezza del datore di lavoro. Lookout fornisce la presente Informativa sulla privacy aziendale ("Informativa") per illustrare le prassi di trattamento adottate per i dati in relazione all'applicazione Lookout for Work ("Servizi"). La presente Informativa regola i dati riguardanti l'utente, raccolti da Lookout dall'utente stesso, tramite l'installazione e l'attivazione dei Servizi sul dispositivo mobile dell'utente. Scaricando e attivando i Servizi, l'utente accetta le modalità di raccolta, utilizzo, divulgazione e archiviazione dei propri dati descritte nella presente Informativa. Tutte le informazioni raccolte da Lookout da fonti diverse dai Servizi sono soggette a un'altra informativa sulla privacy.

Il motivo per cui sono stati scaricati e installati i Servizi può includere istruzioni aziendali fornite ai dipendenti dalla società per cui lavorano, le quali (1) richiedono che alcuni dipendenti o tutto il personale installi i Servizi o (2) che alcuni dipendenti o tutto il personale installi una suite per la gestione dei dispositivi mobili comprensiva dei Servizi. Si tenga presente che, salvo diversamente specificato, questa Informativa regola esclusivamente le prassi di trattamento delle informazioni da parte di Lookout in relazione ai Servizi. Per sottoporre domande o richieste riguardanti la raccolta, l'utilizzo e la divulgazione dei dati e le prassi di sicurezza del datore di lavoro ("Datore di lavoro") o di un Fornitore di soluzioni per la gestione dei dispositivi mobili ("Fornitore di soluzioni MDM"), o per informazioni sui dati raccolti da Lookout per conto del Datore di lavoro, si invita l'utente a rivolgersi alle parti interessate.

Lookout si riserva il diritto di modificare la presente Informativa in qualunque momento, in base a modifiche apportate alla legge, cambiamenti nelle proprie prassi di raccolta e utilizzo dei dati, caratteristiche dei Servizi o avanzamenti tecnologici. Lookout si adopererà per informare gli utenti in caso di variazioni sostanziali della presente Informativa. Se l'utente nutre delle obiezioni nei confronti delle informazioni contenute nel presente documento, deve cessare l'utilizzo dei Servizi.

Lookout ha strutturato la presente Informativa in modo da rispondere ad alcune domande di carattere generale degli utenti relative ai Servizi, che sono elencate di seguito:

1. **Che cos'è l'app Lookout for Work?**
2. **Quali dati vengono raccolti da Lookout dai dispositivi mobili degli utenti?**
3. **Lookout legge o controlla le e-mail degli utenti o visualizza le foto?**
4. **Lookout raccoglie altri dati sugli utenti al di fuori dei loro dispositivi mobili?**
5. **Quando Lookout raccoglie dati dai dispositivi mobili degli utenti?**
6. **In che modo Lookout utilizza i dati raccolti dai dispositivi mobili degli utenti?**
7. **Lookout condivide i dati degli utenti con altri?**
8. **Lookout vende le informazioni personali degli utenti a terzi?**
9. **Quali informazioni NON è in grado di vedere il Datore di lavoro?**
10. **Lookout utilizza i dati degli utenti a fini di marketing?**
11. **In che modo Lookout protegge i dati degli utenti e per quanto li conserva?**
12. **Dove Lookout memorizza i dati degli utenti?**
13. **Che diritti hanno gli utenti in relazione ai propri dati e quali sono le scelte disponibili?**
14. **In che modo gli utenti possono contattare Lookout per sottoporre altre domande?**

1. Che cos'è l'app Lookout for Work?

L'app Lookout for Work è una soluzione di sicurezza per la protezione di sistemi mobili e aziende nei confronti di minacce e violazioni della conformità alle politiche aziendali. Grazie a una rete globale costituita da oltre 100 milioni di sensori, Lookout fornisce una sicurezza predittiva sfruttando l'intelligenza artificiale per identificare complessi schemi di rischio che altrimenti sfuggirebbero ad analisti umani. Quando viene rilevata una minaccia, Lookout fornisce a dipendenti e amministratori opzioni per rimediare (ad esempio, disinstallare un'app o richiedere l'accesso condizionale).

2. Quali dati vengono raccolti da Lookout dai dispositivi mobili degli utenti?

Per proteggere il proprio dispositivo mobile e il Datore di lavoro dalle minacce, Lookout raccoglie dal dispositivo dati appartenenti a determinate categorie, **fra cui**:

- **Dati analitici**, utilizzati per analizzare le prestazioni del prodotto sul dispositivo dell'utente;
- **Dati delle applicazioni**, compresi metadati di tutte le applicazioni installate sul dispositivo mobile (inclusi, senza limitazioni, i nomi delle app e le relative versioni); in alcune circostanze, Lookout può acquisire anche una copia dell'applicazione;
- **Dati di configurazione**, ad esempio se il dispositivo consente l'accesso alla root o se le limitazioni hardware sono state rimosse;
- **Dati del dispositivo**, compresi l'identificativo e le informazioni relative all'operatore MDM;
- **Dati relativi al firmware e al sistema operativo**, compresi produttore e modello del dispositivo, alcune caratteristiche tecniche (fra cui le dimensioni del display e la versione del firmware), il tipo di sistema operativo e la versione;
- **Dati di identificazione,** come l'indirizzo e-mail aziendale, sono raccolti su base opzionale, a meno che il datore di lavoro non utilizzi la funzione di controllo della privacy inclusa nei Servizi;
- **Dati di rete**, compresi metadati relativi alle reti alle quali si connette il dispositivo mobile (inclusi, senza limitazioni, il SSID della rete o l'indirizzo MAC/BSSID univoco dell'apparecchiatura di rete) e l'indirizzo IP (dal quale si possono estrapolare il paese e dati di geolocalizzazione);
- **Dati relativi ai contenuti web,** compresi URL e domini per l'identificazione di contenuti dannosi e contenuti che necessitano di ulteriori analisi.

Si segnala che Lookout necessita di determinati tipi di informazioni per fornire i Servizi agli utenti. Se l'utente non le fornisce o ne richiede la cancellazione, potrebbe non essere più in grado di accedere ai Servizi.

3. Lookout legge o controlla le e-mail degli utenti o visualizza le foto?

No. Lookout raccoglie soltanto i metadati delle applicazioni presenti sul dispositivo o acquisisce l'applicazione in sé. Non vengono raccolti i dati immessi nelle applicazioni dagli utenti. Di conseguenza, Lookout non raccoglie, legge, analizza o esegue la scansione di e-mail o messaggi di testo presenti nel dispositivo, tuttavia potrebbe sottoporre a scansione foto o video in locale sul dispositivo per proteggere l'utente da determinate minacce.

4. Lookout raccoglie altri dati sugli utenti al di fuori dei loro dispositivi mobili?

Il Datore di lavoro può fornire a Lookout l'indirizzo e-mail dell'utente per abilitare i Servizi. Se i Servizi sono integrati con una soluzione MDM ed è attivato il controllo della privacy, Lookout non raccoglie l'indirizzo e-mail dell'utente, sebbene Lookout possa accedere a tale indirizzo e-mail tramite MDM.

Se i Servizi sono stati installati unitamente al prodotto di un Fornitore di soluzioni MDM, Lookout può raccogliere o avere accesso anche a informazioni relative all'utente da tale fornitore, tra cui ad esempio l'indirizzo e-mail.

Contattare il Fornitore di soluzioni MDM per informazioni sulle prassi che adotta in materia di privacy.

Lookout può inoltre raccogliere altre informazioni sull'utente se questo le fornisce direttamente a Lookout contattando l'Azienda e comunicandole volontariamente.

5. Quando Lookout raccoglie dati dai dispositivi mobili degli utenti?

Dopo che l'utente ha scaricato, installato e attivato i Servizi, Lookout inizierà immediatamente a raccogliere dati dal dispositivo per individuare eventuali minacce e verificare la conformità alle politiche aziendali. Quando l'utente installa o accede ad applicazioni sul proprio dispositivo mobile, Lookout ne esegue la scansione alla ricerca di potenziali minacce per la sicurezza.

6. In che modo Lookout utilizza i dati raccolti dai dispositivi mobili degli utenti?

Lookout utilizza le informazioni raccolte per diverse finalità professionali e commerciali. Ad esempio, i dati che vengono raccolti dai dispositivi mobili consentono a Lookout di individuare minacce per gli utenti e/o il Datore di lavoro e permettono all'Azienda di migliorare i Servizi o altri prodotti e offerte. I dati raccolti dai dispositivi mobili degli utenti possono inoltre essere uniti a quelli raccolti da terze parti al fine di migliorare i Servizi. Tali dati vengono anonimizzati. Se i risultati delle analisi effettuate da Lookout vengono condivisi pubblicamente, la pubblicazione avviene con dati aggregati e anonimizzati per proteggere la privacy degli utenti e del Datore di lavoro. Di seguito sono elencate le modalità di utilizzo delle informazioni fornite dagli utenti in base al tipo di dati:

- **Dati delle applicazioni.** Lookout utilizza questi dati per l'erogazione dei Servizi effettuando scansioni dei file delle applicazioni, al fine di stabilire se qualcuna di esse presenti un comportamento anomalo. Quando vengono analizzate le applicazioni presenti sul dispositivo mobile e viene individuata un'applicazione non analizzata in precedenza, Lookout può scaricarne una copia integrale o parziale per verificarla e stabilire se presenti dei rischi, in base alla configurazione dei Servizi stabilita dal Datore di lavoro. Come indicato nella Sezione 3, Lookout non raccoglie i dati immessi dagli utenti nelle applicazioni quando ne scarica una copia.
- **Dati di configurazione.** Lookout analizza i dati di configurazione del dispositivo dell'utente per determinare se è stato modificato, compromesso o configurato in modo non sicuro, ad esempio se è infetto, se sono stati eseguiti processi di rooting o jailbreak o non è stato impostato il codice di accesso.
- **Dati del dispositivo.** Lookout utilizza gli identificativi del dispositivo e dell'operatore MDM per abbinarlo a un sistema terzo, ad esempio una soluzione per la gestione dei dispositivi mobili, in modo da poter segnalare a quel sistema le eventuali minacce rilevate.
- **Dati relativi al firmware e al sistema operativo.** Lookout utilizza queste informazioni per identificare i firmware e i sistemi operativi compromessi e segnalare gli aggiornamenti di sicurezza disponibili per il dispositivo.
- **Dati di identificazione.** Lookout raccoglie, su base opzionale, gli indirizzi e-mail aziendali per fornire informazioni contestuali al Datore di lavoro circa le minacce riscontrate nei dispositivi degli utenti. L'Azienda non invierà mai delle e-mail senza il consenso dell'utente.
- **Dati di rete.** Gli autori degli attacchi possono utilizzare le connessioni Internet, compreso il Wi-Fi, per impossessarsi dei dati, il cosiddetto "attacco man in the middle" (MitM). Per identificare questo tipo di minaccia, Lookout utilizza il nome della rete Wi-Fi (SSID) e stabilisce approssimativamente il paese e la regione dell'utente tramite l'indirizzo IP, senza leggere, memorizzare o trasferire i dati della posizione (GPS) effettiva del dispositivo. I dati vengono anonimizzati e conservati in forma aggregata per ottenere informazioni sulla diffusione di un'applicazione in ogni regione e per effettuare l'analisi delle minacce mobile. Tali informazioni rimarranno anonimizzate per garantire la riservatezza dei dati.
- **Dati relativi ai contenuti web.** Lookout utilizza un'interfaccia VPN per analizzare il traffico web sui dispositivi alla ricerca di minacce nell'ambito della funzione di esplorazione sicura, per bloccare l'accesso a siti web dannosi o di phishing. Contenuti e cronologia non saranno condivisi con il Datore di lavoro, il quale verrà informato solo in caso di minacce rilevate.

In conformità al Regolamento generale sulla protezione dei dati, le basi legali per l'utilizzo delle informazioni degli

utenti a cui si fa riferimento nella presente Informativa dipendono dai rapporti con il Datore di lavoro e dal relativo caso d'uso e possono includere quanto segue: (a) è necessario utilizzare le informazioni personali dell'utente per adempiere gli obblighi di un contratto con esso stipulato (ad esempio, per il Datore di lavoro, per adempiere il contratto di lavoro o, per Lookout, per ottemperare alle Condizioni del servizio, che l'utente accetta scaricando e utilizzando le app Lookout) oppure (b) laddove non sia necessario utilizzare le informazioni dell'utente per l'esecuzione di un contratto, il loro utilizzo è giustificato da interessi legittimi di Lookout, del Datore di lavoro o di altri (ad esempio, per garantire la sicurezza dei Servizi, per gestire i Servizi, per garantire la sicurezza dell'ambiente di lavoro per il personale di Lookout, del Datore di lavoro e di altri, per effettuare e ricevere pagamenti, per prevenire le frodi e per conoscere il cliente al quale vengono forniti i Servizi) e per la conformità a requisiti di legge, ad esempio quelli che prescrivono un'adeguata sicurezza dei dati.

7. Lookout condivide i dati degli utenti con altri?

Poiché si tratta di un prodotto aziendale, alcuni dati vengono condivisi con il Datore di lavoro degli utenti o con altri da esso autorizzati a visualizzarli. Tramite il dashboard dei Servizi, i Datori di lavoro e le relative persone autorizzate possono accedere ad alcune informazioni legate alla sicurezza dei dispositivi mobili degli utenti. Il Datore di lavoro potrebbe avere accesso a informazioni sul dispositivo, quali il modello e l'operatore di telefonia e avere visibilità delle applicazioni identificate come pericolose da Lookout, oltre che di quelle che violano le politiche aziendali applicabili. Per informazioni sulle implicazioni di tali violazioni delle politiche aziendali contattare il Datore di lavoro.

Se i Servizi sono stati installati e attivati unitamente al prodotto di un Fornitore di soluzioni MDM, Lookout può condividere con tale fornitore lo stato di sicurezza e attivazione del dispositivo mobile.

Lookout può condividere dati correlati all'utente con terze parti, inclusi altri membri del proprio gruppo aziendale e fornitori di servizi o partner ingaggiati per eseguire da parte sua funzioni connesse allo svolgimento delle attività aziendali. Possono essere inclusi fornitori di servizi che: (a) forniscono supporto tecnico, operativo o ai clienti, (b) evadono gli ordini e le richieste degli utenti o del Datore di lavoro, (c) ospitano i Servizi, (d) gestiscono database, (e) analizzano i dati al fine di migliorare e innovare il prodotto e (f) supportano altrimenti o commercializzano i Servizi o altri prodotti Lookout. Lookout ha la facoltà di divulgare dati correlati agli utenti a seguito di citazioni in giudizio, ingiunzioni del tribunale o altri procedimenti legali, nonché per affermare o esercitare i propri diritti o difendersi da controversie legali. Qualora Lookout dovesse ricevere una richiesta di informazioni da un'autorità locale, statale, federale o straniera, cercherà di trasmetterla al Datore di lavoro affinché la elabori, ma si riserva il diritto di rispondere direttamente e fornire le informazioni richieste se ritiene che tale risposta sia adeguata dal punto di vista legale. Lookout ha la facoltà di divulgare dati correlati agli utenti se ritiene in buona fede che ciò sia necessario per indagare, prevenire e contrastare possibili attività illegali, sospette frodi, situazioni che comprendono potenziali minacce alla sicurezza fisica di persone, violazioni della presente Informativa, del Contratto di licenza o del Contratto con l'utente finale relativi ai Servizi e/o per proteggere i diritti e le proprietà di Lookout o dei suoi dipendenti e utenti o del pubblico. A questo fine potrebbe dover comunicare le informazioni degli utenti alle forze dell'ordine, a enti governativi, a tribunali e/o ad altre organizzazioni.

Lookout può condividere dati legati agli utenti in seguito a fusioni, riorganizzazioni, vendita totale o parziale dei propri beni, finanziamento o acquisizione della sua attività, anche parziale, da parte di un'altra società.

8. Lookout vende le informazioni personali degli utenti a terzi?

No. Lookout non vende le informazioni personali (per come intendiamo il termine ai sensi del California Consumer Privacy Act) dei suoi utenti. Come già detto in precedenza nella Sezione 6, abbiamo la facoltà di aggregare i dati raccolti dai dispositivi mobili degli utenti a quelli raccolti da terze parti al fine di migliorare i Servizi. Tali dati, tuttavia, sono pseudonimizzati e non contengono informazioni personali.

9. Quali informazioni NON è in grado di vedere il Datore di lavoro?

Lookout condivide con i Datori di lavoro soltanto le informazioni necessarie a confermare l'assenza di eventuali

minacce e a verificare la conformità alle politiche di sicurezza aziendali. Ad esempio, Lookout non consente al Datore di lavoro di vedere il contenuto delle e-mail, la cronologia di esplorazione, i contatti, il calendario, i messaggi di testo e le app sicure installate (a meno che l'utilizzo di tali app non violi le politiche aziendali applicabili del Datore di lavoro) né di tracciare la posizione dell'utente.

10. Lookout utilizza i dati degli utenti a fini di marketing?

Lookout non utilizza i dati raccolti dal dispositivo mobile con sistemi automatizzati per vendere prodotti all'utente e non li condivide con terze parti per scopi di marketing di queste ultime. Lookout ha la facoltà di aggregare le informazioni raccolte dal dispositivo per svolgere ricerche e fornire informazioni sulla sicurezza e le minacce del dispositivo mobile. In queste circostanze, le informazioni aggregate incluse nella ricerca sono anonimizzate.

11. In che modo Lookout protegge i dati degli utenti e per quanto li conserva?

Lookout ha implementato ragionevoli misure di sicurezza, di natura tecnica e amministrativa, nonché fisiche, per la protezione dall'accesso, dalla distruzione o dalla modifica non autorizzati delle informazioni degli utenti. Questi sistemi di prevenzione, tecnologicamente all'avanguardia, sono stati espressamente messi in atto per proteggere le informazioni sensibili raccolte, trattate e archiviate da Lookout.

Sebbene Lookout adotti misure adeguate per proteggere le informazioni dalla divulgazione non autorizzata, poiché nessun metodo di trasmissione via Internet o di archiviazione elettronica è sicuro al 100%, Lookout non è in grado di assicurare che le informazioni che raccoglie non vengano mai divulgate in modi non coerenti con la presente Informativa.

La politica di Lookout in materia di conservazione dei dati personali prevede che questi vengano mantenuti soltanto per il tempo ragionevolmente necessario a fornire i Servizi agli utenti e ad altri, salvo se diversamente richiesto per ottemperare a obblighi di legge. Lookout si riserva la facoltà di cancellare i dati dell'utente dopo 60 giorni se l'account è inattivo e secondo quanto disposto nelle Condizioni del servizio. Le informazioni possono essere conservate in copie create a scopo di backup e per finalità di continuità aziendale. In questo caso, tutti i dati inattivi sono protetti con crittografia a 256 bit.

12. Dove Lookout memorizza i dati degli utenti?

Lookout è un'azienda con sede a San Francisco e server fisicamente ubicati negli Stati Uniti. I Dati personali raccolti da utenti residenti al di fuori degli Stati Uniti verranno trasferiti negli USA. Se i Servizi vengono utilizzati esternamente agli Stati Uniti, le informazioni possono essere trasferite, memorizzate ed elaborate negli USA, luogo in cui sono ubicati e gestiti i server di Lookout. Le informazioni possono anche essere trasferite in altri stati dove Lookout o sue affiliate, controllate e i suoi fornitori di servizi gestiscono delle strutture.

Questi stati possono avere leggi sulla protezione dei dati diverse da quelle dello stato dell'utente e in alcuni casi possono non garantire un livello di protezione così elevato. Tuttavia, ovunque le informazioni dell'utente vengano trasferite ed elaborate, Lookout adotta misure per garantire che i Dati personali siano protetti in conformità alla presente Informativa e alle leggi in materia di protezione dei dati. Se gli utenti sono residenti dello Spazio economico europeo ("SEE"), del Regno Unito o della Svizzera, Lookout adotta una varietà di meccanismi legali che aiutano a garantire la protezione dei loro Dati personali e dei loro diritti, incluso le clausole contrattuali standard approvate dalle Commissioni Europee per il trasferimento dei dati personali in Stati terzi.

Lookout è una società autocertificata presso il Dipartimento del commercio statunitense come aderente alle direttive del Privacy Shield fra UE e USA e Svizzera e USA per quanto riguarda la raccolta, l'uso e la conservazione dei Dati personali di soggetti residenti negli Stati dell'Unione Europea, nel Regno Unito e in Svizzera. Queste direttive sono state sviluppate per consentire alle aziende di rispettare i requisiti di protezione dei dati nel trasferimento di informazioni personali dall'Unione Europea, dal Regno Unito e dalla Svizzera agli Stati Uniti. Per ulteriori informazioni sul Privacy Shield e per visualizzare la certificazione di Lookout come aderente al Privacy Shield, visitare il sito http://www.privacyshield.gov.

In quanto entità certificata, Lookout aderisce ai principi del Privacy Shield per quanto riguarda i requisiti di protezione dei dati nel trasferimento di informazioni personali dall'Unione Europea, dal Regno Unito e dalla Svizzera agli Stati Uniti. Come richiesto da questi principi, quando Lookout riceve informazioni ai sensi del Privacy Shield e le trasferisce a fornitori di servizi terzi operanti in qualità di agenti per conto di Lookout, quest'ultima è vincolata da determinate responsabilità se (i) l'agente tratta le informazioni in modo non coerente con i principi del Privacy Shield e (ii) Lookout è responsabile dell'evento che ha dato origine al danno.

Per domande o reclami inerenti alle prassi relative alla privacy di Lookout, incluse domande sul Privacy Shield, è possibile contattare Lookout utilizzando l'indirizzo e-mail o l'indirizzo postale indicati in "Come contattare Lookout per sottoporre richieste o domande". Lookout fornirà la sua collaborazione per risolvere il problema.

13. Che diritti hanno gli utenti in relazione ai propri dati e quali sono le scelte disponibili?

In conformità con il Regolamento generale sulla protezione dei dati ("GDPR"), i residenti dello Spazio economico europeo ("SEE"), del Regno Unito o della Svizzera, sono titolari dei diritti descritti qui di seguito:

- **Accesso.** L'utente ha il diritto di richiedere una copia dei Dati personali in corso di trattamento. La richiesta di copie multiple può essere subordinata al pagamento di un compenso ragionevole;
- **Rettifica.** L'utente ha il diritto di richiedere la correzione di qualsiasi errore nei Dati personali, siano essi incompleti o inesatti, di cui Lookout è in possesso;
- **Cancellazione.** L'utente ha il diritto di richiedere la cancellazione dei Dati personali che lo riguardano in determinate situazioni, come ad esempio quando non sono più necessari o il consenso viene revocato (ove applicabile);
- **Portabilità.** L'utente ha il diritto di ricevere i propri Dati personali forniti a Lookout in un formato strutturato, comune e leggibile meccanicamente, nonché il diritto di trasmettere tali dati a terze parti in determinate situazioni;
- **Obiezione.** L'utente ha il diritto di (i) opporsi in qualsiasi momento al trattamento dei Dati personali per scopi di marketing diretto e (ii) opporsi al trattamento dei Dati qualora il motivo legale di tale trattamento sia necessario per il perseguimento di interessi legittimi di Lookout o di terzi;
- **Limitazione.** L'utente ha il diritto di richiedere la limitazione del trattamento dei suoi Dati personali in determinate circostanze, ad esempio quando ne contesta l'esattezza;
- **Revoca del consenso.** Il trattamento dei Dati personali da parte di Lookout ha come base legale il consenso (o consenso esplicito) degli utenti, i quali hanno il diritto di revocare tale consenso in qualsiasi momento.

Gli utenti che desiderano esercitare tali diritti devono contattare il Datore di lavoro. Qualora Lookout agisca in qualità di responsabile del trattamento dei Dati personali, è inoltre possibile contattare l'Azienda utilizzando le informazioni per i contatti riportate di seguito. In circostanze adeguate, Lookout può inoltrare la richiesta al Datore di lavoro e seguire le sue istruzioni per gestirla. L'Azienda si impegna a rispondere puntualmente alle richieste e comunque non oltre entro 30 giorni. In determinate situazioni, tuttavia, Lookout potrebbe non essere in grado di consentire l'accesso o la cancellazione dei Dati personali degli utenti che detiene.

I residenti del SEE, del Regno Unito e della Svizzera che non sono soddisfatti della gestione delle problematiche relative alle procedure di Lookout in materia di privacy possono richiedere gratuitamente ulteriore assistenza al meccanismo di ricorso indipendente designato da Lookout ai sensi del Privacy Shield, relativamente al quale è possibile trovare ulteriori informazioni sul sito https://www.jamsadr.com/eu-us-privacy-shield. Hanno inoltre il diritto di presentare un reclamo presso l'autorità di controllo preposta. Si invitano tuttavia gli utenti a rivolgersi prima a Lookout, che farà del suo meglio per risolvere il problema. I residenti nell'Unione Europea possono anche decidere di ricorrere all'arbitrato vincolante per appianare controversie non risolte, tuttavia sono prima tenuti a: (1) contattare Lookout e darle la possibilità di risolvere la questione; (2) richiedere l'assistenza del meccanismo di ricorso indipendente designato da Lookout, come descritto in precedenza e (3) contattare il Dipartimento del commercio statunitense (direttamente o tramite un'autorità garante per la protezione dei dati europea) e concedergli del tempo

per tentare di risolvere la questione. Per ulteriori informazioni sul sistema di arbitrato vincolante del Privacy Shield, consultare il sito https://www.privacyshield.gov/article?id=ANNEX-I-introduction. Ciascuna delle parti sosterrà le proprie spese legali. Si ricorda che, ai sensi del Privacy Shield, gli arbitri possono imporre esclusivamente rimedi equi, non monetari, specifici in base all'interessato, necessari per rimediare a una violazione dei principi del Privacy Shield in relazione alla persona. Lookout è soggetta alle indagini e al potere esecutivo della Commissione federale per il commercio statunitense (Federal Trade Commission, FTC).

Gli utenti potrebbero godere di determinati diritti in base alla legge applicabile, compreso il Regolamento generale sulla protezione dei dati and the California Consumer Privacy Act. Coloro che desiderano esercitare tali diritti devono contattare il Datore di lavoro. È inoltre possibile contattare Lookout utilizzando le informazioni per i contatti riportate di seguito.

14. In che modo gli utenti possono contattare Lookout per sottoporre altre domande?

Per ulteriori informazioni, si invita a contattare il Datore di lavoro. È inoltre possibile rivolgere domande al Responsabile della protezione dei dati di Lookout, scrivendo all'indirizzo e-mail privacy@lookout.com o utilizzando l'indirizzo postale di Lookout, Inc., Att.: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA 02108. I residenti del SEE possono inoltre scrivere all'indirizzo postale di Lookout, Inc., Att: Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem, Paesi Bassi.