Lookout, Inc.
App Lookout Personal
Informativa sulla privacy

Data di efficacia: 01/01/2020
Data origine: 15/11/2016
Data revisione: 1/1/2023

1. Introduzione

Il presente documento costituisce l'Informativa sulla privacy di Lookout ("Informativa") relativa all'app Lookout Personal ("app Personal") e spiega quali informazioni raccoglie l'Azienda durante l'utilizzo dell'app e come vengono impiegate. È importante leggere l'Informativa unitamente alle Condizioni del servizio di Lookout (disponibili sul sito www.lookout.com/legal/terms) in quanto entrambi i documenti si riferiscono all'utilizzo dell'app Lookout Personal da parte dell'utente. Tutte le informazioni raccolte da Lookout da fonti diverse dall'app Personal sono soggette a un'altra informativa sulla privacy.

È possibile che la presente Informativa venga rivista e adeguata in base alle modifiche dei prodotti e dei servizi Lookout e alle leggi applicabili sia a Lookout che agli utenti. Gli utenti verranno informati in caso di variazioni sostanziali della presente Informativa. Se non si desidera che le informazioni siano soggette all'Informativa rivista, si dovrà chiudere l'account.

È possibile accedere alla presente Informativa dalla schermata di login dell'applicazione per dispositivi mobili Lookout, dalle impostazioni dell'app Personal e dal sito web dell'Azienda.

2. Informazioni raccolte dall'Azienda

L'app Lookout Personal fornisce vari livelli di offerte. Ogni livello consente l'accesso a funzionalità di sicurezza di Lookout di grado crescente. Le informazioni necessarie per fornire questi servizi possono variare e sono riportate in questo documento a vantaggio dell'utente, affinché sia a conoscenza di quali informazioni vengono raccolte direttamente dalla persona e dal dispositivo, e delle modalità con cui Lookout le utilizza. Per ulteriori informazioni sulle funzionalità dell'app Personal per dispositivi iOS e Android vedere https://www.lookout.com/products/personal/ios e https://www.lookout.com/products/personal/android.

a. Categorie di informazioni. Lookout o suoi i partner possono raccogliere le seguenti categorie di informazioni dall'utente nel corso dell'utilizzo dell'app Personal:

i. ***Dati di registrazione***, compresi indirizzo e-mail e password.

ii. ***Dati del dispositivo***, compresi identificativo dell'apparecchiatura (ad es., il numero di cellulare, il tipo di dispositivo e il produttore), il tipo di sistema operativo e la versione, l'operatore/provider del servizio di telefonia mobile utilizzato, il tipo di rete, il paese di origine, il nome della rete Wi-Fi (SSID), l'indirizzo IP (Internet Protocol) e la data e ora delle richieste.

iii. ***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 integrale o parziale dei file dell'applicazione sul dispositivo dell'utente se viene individuata un'applicazione non analizzata in precedenza. Questi dati sono anonimizzati e conservati in forma aggregata per garantire che non sia possibile distinguere un singolo individuo dagli altri clienti. Lookout può inoltre raccogliere informazioni sul comportamento delle applicazioni presenti sul dispositivo (ad es., se un'applicazione invia messaggi di testo premium che possono comportare l'addebito di costi nella bolletta telefonica) e sui servizi di rete con cui comunicano le applicazioni.

iv. ***Dati della posizione.*** Alcune funzioni offrono prestazioni migliori se è possibile identificare la posizione del dispositivo mobile. Con il consenso dell'utente, che viene fornito durante la registrazione iniziale, Lookout raccoglie le informazioni sulla posizione in due modi: ricevendole direttamente dal dispositivo portatile o, in alcune situazioni, ricavando direttamente i dati della posizione dal ripetitore di telefonia oppure dalle informazioni sull'hot-spot Wi-Fi. Per convertire questi dati in informazioni sulla posizione utilizzabili, Lookout può ricorrere a fornitori di servizi terzi. Per evitare la condivisione dei dati sulla posizione, accedere alle impostazioni del dispositivo portatile e disattivare i servizi di geolocalizzazione. Tuttavia, questo potrebbe limitare le prestazioni delle app Lookout.

v. ***Dati relativi agli avvisi di furto***, compresi dati di posizione e una fotografia scattata quando gli avvisi di furto vengono attivati.

vi. ***Dati di pagamento***, compresi i dati della carta di credito come numero della carta, data di scadenza, codice di sicurezza e altre informazioni necessarie per la fatturazione. Se si acquista la versione Premium o Premium Plus dell'app, i dati potrebbero essere raccolti direttamente dai fornitori terzi di Lookout.

vii. ***Dati relativi ai contenuti web,*** compresi URL e domini per l'identificazione di contenuti dannosi e contenuti che necessitano di ulteriori analisi per stabilire se tali URL presentino problemi di sicurezza (ad es., se possano veicolare attacchi di phishing o contenere malware). Lookout non raccoglie la cronologia di esplorazione.

viii. ***Dati relativi al servizio di protezione per il furto di identità***, che vengono forniti dall'utente in seguito all'acquisto della versione Premium Plus dell'app Lookout. Questi dati includono informazioni private (ad es., numero della patente o della previdenza sociale, numero del passaporto o altri numeri di documenti di identità), informazioni finanziarie (ad es., numero di conto corrente o della carta di debito e credito), numero di assicurazione sanitaria e altri dati personali dell'utente (o di altre persone che l'utente ha iscritto al servizio), compreso nome e titolo, e potrebbero essere raccolti direttamente dal partner di Lookout CSIdentity (acquisito da Experian).

ix. ***Dati analitici,*** compresi quelli provenienti da strumenti di terze parti come Mixpanel, Braze e mParticle, che permettono a Lookout di analizzare e aggregare i dati riguardanti l'utilizzo dei Servizi da parte degli utenti. Per ulteriori informazioni, si rimanda all'Informativa sulla privacy di MixPanel, all'Informativa sulla privacy di Braze e all'Informativa sulla privacy di mParticle.

Poiché le caratteristiche del prodotto variano a seconda del livello, Lookout può raccogliere diversi tipi di informazioni in base al livello che si sta utilizzando, come descritto di seguito.

b. Informazioni raccolte da Lookout per l'app Personal versione base

i. ***Dati di registrazione.*** Per creare un account è necessario fornire un indirizzo e-mail e una password.

ii. ***Dati del dispositivo.*** Quando si usano i servizi Lookout, i server dell'Azienda registrano determinate informazioni relative al dispositivo mobile utilizzato, come descritto in precedenza nella Sezione 2(a)(ii).

iii. ***Dati delle applicazioni.*** Quando si usano i servizi Lookout, l'Azienda raccoglie ed effettua il download di una copia intera o parziale dei file delle applicazioni presenti sul dispositivo, qualora venga individuata un'applicazione non analizzata in precedenza come descritto in precedenza nella Sezione 2(a)(iii). Per chiarezza informativa, si ricorda che 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.

iv. ***Dati della posizione.*** Quando è attiva, la funzione di smarrimento del dispositivo di Lookout, compresa la capacità di individuarlo da remoto e attivare sul dispositivo una sirena d'allarme, utilizza i dati della posizione per aiutare l'utente a individuare il telefono nelle vicinanze dell'ultima destinazione nota in caso di smarrimento ed esaurimento della batteria. Se la funzione di inseguimento del segnale è abilitata, quando la batteria sta per esaurirsi vengono raccolte e inviate a Lookout informazioni sulla posizione del dispositivo.

c. Informazioni raccolte da Lookout per l'app Personal versione Premium

Lookout raccoglie le stesse informazioni indicate per l'app Personal versione base; in aggiunta, il partner di Lookout raccoglie anche i dati di pagamento direttamente dall'utente per consentire l'accesso alle funzioni premium, i dati relativi ai contenuti Web per la funzione di esplorazione sicura e i dati relativi agli avvisi di furto per consentire l'utilizzo di questa funzione come descritto di seguito.

i. ***Dati di pagamento.*** Se si acquista un abbonamento ai servizi Lookout Premium o Premium Plus direttamente da Lookout, per l'elaborazione dei pagamenti viene utilizzato un fornitore terzo che raccoglie i dati di pagamento. Il fornitore terzo utilizzerà queste informazioni per la fatturazione dei servizi e Lookout riceverà le informazioni relative all'account Premium e/o Premium Plus dell'utente. Tali informazioni includeranno l'importo pagato e il metodo di pagamento. A Lookout non perverranno informazioni bancarie o relative alla carta di credito dell'utente, che rimarranno esclusivamente al fornitore terzo incaricato dell'elaborazione dei pagamenti. Se l'app Lookout viene acquistata su un App Store o tramite il piano tariffario del provider di telefonia, le informazioni relative al pagamento saranno gestite dall'App Store o dal provider. Il pagamento non passa da Lookout e può essere

elaborato in vari modi. Affinché i servizi possano essere erogati all'utente, l'App Store invierà conferma dell'acquisto a Lookout. I provider di telefonia possono condividere informazioni quali numero di telefono, ID abbonato, codice prodotto e altri dati dell'utente di natura non finanziaria. L'App Store e il provider di telefonia non condividono i dati della carta di credito o di fatturazione. Per ulteriori informazioni fare riferimento alle politiche e alle procedure di elaborazione pagamenti dell'App Store o del provider di telefonia.

ii. ***Dati relativi ai contenuti web.*** Per fornire il servizio di esplorazione sicura, Lookout utilizza dati relativi ai contenuti web. Se non si desidera che vengano registrati gli URL non sicuri visitati, è possibile disattivare la funzione di esplorazione sicura; tutte le altre funzioni di Lookout rimarranno operative.

iii. ***Dati relativi agli avvisi di furto.*** Quando sono attivati gli avvisi di furto, viene scattata una foto. L'immagine e i dati relativi alla posizione (GPS) vengono memorizzati per breve tempo sui server di Lookout in modo da poter inviare all'utente un'e-mail con l'immagine e la mappa con la posizione del dispositivo. L'immagine viene in seguito cancellata dal server di Lookout. L'e-mail viene inviata all'indirizzo associato all'account, per cui è importante mantenerlo aggiornato utilizzando le impostazioni dell'account.

d. Informazioni raccolte da Lookout per l'app Personal versione Premium Plus

Lookout raccoglie le stesse informazioni indicate per l'app Personal versione Premium; in aggiunta, il partner di Lookout raccoglie anche i dati relativi al servizio di protezione per il furto di identità.

i. ***Dati relativi al servizio di protezione per il furto di identità.*** Nell'ambito di questa funzione, l'utente potrebbe fornire i dati descritti in precedenza per usufruire di alcuni servizi di protezione dell'identità forniti dal partner di Lookout CSIdentity (acquisito da Experian). Le informazioni che CSIdentity raccoglie e memorizza dipendono dai dati inseriti nell'app Personal. Per poter garantire i propri servizi, CSIdentity ha la necessità di trasmettere i dati relativi alla protezione dell'identità dell'utente a fornitori terzi (quali società di verifica dell'identità, agenzie di rilevazione dei consumatori, istituti di credito, società di accertamento creditizio, autorità preposte all'applicazione delle leggi e altri).

e. Informazioni che Lookout raccoglie da fonti terze

Lookout riceve dati analitici da terze parti secondo le modalità descritte in precedenza.

3. Modalità di utilizzo delle informazioni degli utenti

Quando Lookout raccoglie informazioni dagli utenti, le memorizza e le associa all'account utente, salvo se diversamente indicato. Si segnala che Lookout necessita di determinati tipi di informazioni per fornire i servizi agli utenti. Se l'utente non le fornisce o chiede di cancellarle, potrebbe non essere più in grado di accedere ai servizi Lookout. Lookout tiene in seria considerazione la privacy degli utenti e utilizza e divulga queste informazioni esclusivamente ai fini professionali e commerciali descritti nella presente Informativa. Di seguito sono elencate le modalità di utilizzo delle informazioni fornite dagli utenti in base al tipo di dati:

a. 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. 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. Le informazioni ricavate da tale analisi rimarranno anonimizzate per garantire la riservatezza dei dati. L'unione dei dati dei clienti effettuata in modo sicuro e riservato permette a Lookout di identificare meglio le minacce in circolazione e di migliorare i servizi offerti.

b. Dati del dispositivo. Periodicamente possono essere effettuate scansioni del dispositivo al fine di raccogliere informazioni sulle applicazioni, sui file del sistema operativo utilizzato, nonché sul dispositivo stesso. Lookout raccoglie i risultati delle scansioni eseguite mediante i propri servizi e le informazioni più aggiornate sull'assetto di sicurezza del dispositivo. Vengono inoltre eseguiti regolarmente gli aggiornamenti delle definizioni delle minacce. Queste attività contribuiscono a proteggere l'endpoint consentendo all'app Personal di rilevare e risolvere le minacce sul dispositivo mobile. Lookout può inoltre utilizzare le informazioni relative al dispositivo del cliente, se disponibili, per informarlo della necessità di aggiornare il sistema operativo. Oltre a utilizzare le informazioni fornitegli dagli utenti e quelle raccolte autonomamente dall'endpoint mobile al fine di fornire i servizi, Lookout utilizza le informazioni ottenute dai dispositivi degli utenti anche per finalità di analisi dei dati.

Queste analisi forniscono informazioni importanti, utili per migliorare le funzioni e facilitare l'uso dei prodotti dell'Azienda. Lookout analizza informazioni quali la frequenza con cui l'applicazione Lookout viene utilizzata, gli eventi che si verificano all'interno dell'applicazione e l'origine da cui l'applicazione Lookout è stata scaricata sul dispositivo endpoint mobile. Queste informazioni vengono inoltre utilizzate dall'Azienda in forma aggregata per eseguire l'analisi di minacce già note o nuove per i sistemi mobili.

c. ***Dati relativi al servizio di protezione per il furto di identità.*** CSIdentity utilizza tali informazioni per verificare l'identità dell'utente e fornire i servizi di protezione dell'identità richiesti. Se si esegue l'upgrade dell'abbonamento a una formula Premium Plus che include l'assicurazione per il furto di identità, le informazioni dell'utente verranno utilizzate dai partner di Lookout per fornirgli l'assistenza e la copertura assicurativa applicabile in caso di compromissione dell'identità.

d. **Dati della posizione.** La funzione di smarrimento del dispositivo di Lookout include la capacità di individuarlo da remoto e attivare sul dispositivo una sirena d'allarme dall'account personale sul sito lookout.com. Lookout utilizza i dati della posizione per aiutare l'utente a individuare il telefono nelle vicinanze dell'ultima destinazione nota in caso di smarrimento ed esaurimento della batteria. Se la funzione di inseguimento del segnale è abilitata, quando la batteria sta per esaurirsi vengono raccolte informazioni sulla posizione del dispositivo, che vengono quindi inviate a Lookout. La posizione del telefono viene salvata sul sito lookout.com nel momento in cui viene ricevuto l'avviso di batteria in esaurimento. È possibile attivare e disattivare questa funzione dalle impostazioni dell'app Personal.

e. **Dati di registrazione.** Lookout può utilizzare l'indirizzo e-mail dell'utente per inviare informazioni relative ad annunci di prodotti e promozioni speciali sia di Lookout che dei suoi business partner. Se l'utente invia un'e-mail a Lookout per richiedere assistenza, Lookout può conservare queste informazioni per fornire il supporto richiesto e migliorare i servizi. Lookout può utilizzare l'indirizzo e-mail dell'utente per comunicare con il dispositivo in merito ai servizi offerti, compreso l'invio di notifiche relative alla privacy o alla sicurezza e per informazioni sulle modifiche sostanziali ai servizi forniti.

f. **Dati relativi agli avvisi di furto.** Queste informazioni vengono utilizzate da Lookout per garantire il servizio di avviso in caso di furto.

g. **Dati relativi ai contenuti web.** La funzione di esplorazione sicura è concepita per identificare gli URL non sicuri e avvertire l'utente, in modo che possa scegliere di non caricarli. Gli URL visitati vengono anonimizzati e inviati a Lookout per l'esecuzione delle scansioni di sicurezza. Le registrazioni degli URL non sicuri visitati dall'utente vengono utilizzate per notificare all'utente che è stato eseguito un tentativo di stabilire una connessione non sicura.

4. Modalità di divulgazione delle informazioni degli utenti

Questa sezione illustra come Lookout condivide e divulga le informazioni degli utenti.

a. **Partner e fornitori di servizi terzi.** Lookout può condividere le informazioni degli utenti con fornitori terzi di prodotti e servizi che si integrano con il software Lookout, i quali hanno la necessità di conoscerle per soddisfare richieste di prodotti o servizi, fornire assistenza o analizzare dati relativi alle prestazioni, nonché per finalità connesse al miglioramento dei prodotti. Ad esempio:

    i. Il partner di Lookout, CSIdentity (acquisito da Experian), raccoglie le informazioni fornite dall'utente nell'ambito della funzione di protezione per il furto di identità, allo scopo di consentire l'erogazione del servizio. CSIdentity può, a sua volta, trasmettere i dati a terze parti (quali società di verifica dell'identità, agenzie di rilevazione dei consumatori, istituti di credito, società di accertamento creditizio, autorità preposte all'applicazione delle leggi e altri) al fine di fornire all'utente i servizi richiesti. CSIdentity può inoltre fornire all'utente monitoraggio e avvisi e ottenere informazioni e report relativi all'utente (o altre persone da esso iscritte) nell'ambito della fornitura dei servizi di protezione dell'identità, fra cui cronologia degli indirizzi, nome, alias e altri elementi. Lookout richiede che CSIdentity e i fornitori di servizi di cui si serve utilizzino i dati raccolti dagli utenti esclusivamente ai fini della fornitura di servizi tramite il prodotto Premium Plus dell'app Lookout.

ii. Lookout può condividere le informazioni degli utenti con rivenditori o altri operatori di telefonia mobile per garantire la corretta fornitura dell'acquisto e dei relativi servizi di assistenza, nonché l'esecuzione di funzioni connesse allo svolgimento delle attività aziendali.

iii. Lookout può utilizzare le informazioni dell'utente per svolgere ricerche di mercato e attività promozionali congiunte con società che commercializzano prodotti in grado di offrire valore aggiunto ai prodotti o servizi Lookout (ad esempio, operatori di telefonia mobile).

b. Soggetti partner terzi per le operazioni di pagamento. Lookout può consentire ai fornitori di servizi di raccogliere informazioni direttamente dagli utenti al fine di svolgere attività contabili, di revisione o di riconciliazione contabile e riscossione crediti.

c. Esecuzione degli obblighi di legge. Lookout può divulgare le informazioni degli utenti nel rispetto della legge, ad esempio per: (i) uniformarsi a leggi, regolamenti o procedimenti legali, nonché per soddisfare requisiti di sicurezza nazionale o di applicazione della legge; (ii) proteggere la sicurezza di persone, entità o strutture; (iii) risolvere potenziali violazioni dell'Informativa; (iv) svolgere accertamenti su frodi, questioni di sicurezza o problemi tecnici o (v) proteggere i propri diritti o proprietà o quelli di terze parti, di dipendenti, di utenti o del pubblico. Lookout ritiene che gli utenti abbiano il diritto di sapere se all'Azienda viene richiesto per legge di divulgare informazioni che li riguardano. Pertanto, prima di divulgare informazioni sensibili in ottemperanza a una richiesta delle autorità (ad esempio, a seguito di una citazione in giudizio o ingiunzione del tribunale), l'utente viene informato via e-mail utilizzando l'indirizzo specificato nell'account, a meno che (a) sia fatto divieto a Lookout di procedere in tal senso, (b) si tratti di un caso di emergenza in cui la notifica potrebbe indurre il rischio di lesioni personali o di decesso, o qualora possa comportare danni a minori. Inoltre, nulla di quanto incluso nella presente Informativa deve essere inteso come atto a limitare eventuali difese legali o obiezioni dell'utente nei confronti di terze parti, inclusa la richiesta da parte di autorità governative di divulgare le informazioni dell'utente.

d. Eventuali modifiche all'assetto societario di Lookout. Lookout può inoltre divulgare le informazioni degli utenti a un acquirente effettivo o potenziale (e ai suoi agenti e consulenti) in relazione a qualsiasi acquisto, fusione o acquisizione, effettivo o proposto, di qualsiasi segmento dell'attività, a condizione che l'acquirente sia informato circa le modalità di utilizzo delle informazioni degli utenti ai soli scopi divulgati nella presente Informativa.

e. Dati anonimizzati e aggregati. I dati vengono anonimizzati, aggregati e riepilogati ai fini dell'analisi e possono includere anche informazioni relative agli utenti. Lookout si riserva la facoltà di condividere pubblicamente i report derivanti dalle analisi di questi dati, al fine di diffondere la conoscenza delle minacce per i sistemi mobili e ottenere informazioni sul funzionamento della specifica applicazione per dispositivi mobili.

f. Consenso dell'utente. Lookout può divulgare le informazioni degli utenti anche con terze parti, previo consenso.

5. Scelte degli utenti

a. Possibilità di accedere e aggiornare le impostazioni

Gli utenti possono aggiornare o modificare alcune impostazioni che influiscono sulle modalità di condivisione dei dati con Lookout tramite la pagina delle impostazioni nell'applicazione per dispositivi mobili oppure accedendo al proprio account Lookout sul sito web https://my.lookout.com/user/login. Per proteggere la privacy e la sicurezza dell'utente, sono richiesti nome utente e password al fine di verificarne l'identità prima di consentire l'accesso o di permettere di apportare modifiche all'account.

b. Esclusione dalle e-mail

È possibile chiedere di essere esclusi dalle comunicazioni promozionali di Lookout utilizzando il link per annullare l'iscrizione presente in ogni e-mail. Sebbene le richieste di esclusione vengano di norma elaborate immediatamente, possono occorrere fino a dieci (10) giorni lavorativi affinché la richiesta di cancellazione vada a buon fine. Anche dopo avere richiesto l'esclusione dai messaggi promozionali di Lookout l'utente continuerà a ricevere comunicazioni relative a prodotti e transazioni in merito ai servizi Lookout. È possibile richiedere l'esclusione da alcuni di questi messaggi di notifica agendo sulle impostazioni dell'account.

6. Conservazione dei dati

Lookout conserverà i Dati personali (intesi secondo la definizione data dal GDPR) soltanto per il tempo ragionevolmente necessario a fornire i prodotti e i servizi agli utenti, salvo quando diversamente richiesto per ottemperare a obblighi di legge.

7. Sicurezza

a. Responsabilità di Lookout

Lookout è un'azienda che si occupa di sicurezza, pertanto considera molto importante la protezione dei dati degli utenti e impiega sistemi di prevenzione ragionevoli, disponibili in commercio, di natura fisica, gestionale e tecnologica, per garantire l'adozione di misure tecnico-organizzative adeguate al rischio derivante dal trattamento delle informazioni personali. Ad esempio, per proteggere l'account e i dati degli utenti, utilizza congiuntamente firewall, autenticazione, sicurezza fisica e altre misure di prevenzione. Quando vengono immesse informazioni sensibili (per esempio i dati sulla posizione) nell'applicazione Lookout, queste vengono crittografate con tecnologia SSL (Secure Socket Layer) sia durante il trasferimento che in archivio. Per rafforzare i propri sistemi contro gli attacchi Lookout inoltre esegue test di penetrazione con l'ausilio di terze parti. Lookout adotta tutte le misure ragionevolmente possibili per implementare controlli finalizzati alla protezione da minacce tecnologiche complesse e da altri attacchi criminosi, oltre che per difendersi da eventuali negligenze dei dipendenti.

Poiché nessun metodo di trasmissione via Internet o di archiviazione elettronica è sicuro al 100%, Lookout non è in grado di assicurare o garantire la sicurezza di tutte le informazioni, dei dati o dei contenuti che riceve dagli utenti per gestire i servizi o che gli utenti trasmettono a Lookout. La ricezione o trasmissione delle informazioni dell'utente avviene su base volontaria e quest'ultimo se ne assume i rischi. Lookout non è in grado di garantire che non avverrà alcun accesso alle informazioni e che queste non verranno divulgate, alterate o distrutte in seguito a violazioni delle misure di prevenzione fisiche, tecniche o gestionali.

Qualora Lookout dovesse venire a conoscenza di una violazione della sicurezza, tenterà di notificarlo elettronicamente in modo che gli utenti possano adottare misure di protezione adeguate. Verrà inoltre pubblicato un avviso nei servizi Lookout qualora dovessero verificarsi infrazioni. A seconda del paese in cui risiede l'utente, potrebbe godere del diritto legale di ricevere una notifica scritta in caso di violazioni della sicurezza.

b. Responsabilità dell'utente

L'utente ha la responsabilità di mantenere sempre segreta la propria password. Si consiglia di utilizzare una password sicura non utilizzata per altri servizi. Se si ha il sospetto che la password sia stata compromessa, cambiarla immediatamente tramite il sito web di Lookout oppure contattare Lookout all'indirizzo support@lookout.com per ricevere assistenza. L'utente ha la responsabilità di garantire che l'indirizzo e-mail associato all'account sia corretto, in quanto viene utilizzato per contattarlo in caso di aggiornamenti del servizio, modifiche alle politiche aziendali e attività dell'account quali richieste di dati o tentativi di localizzare il dispositivo dell'utente. Lookout non è responsabile della trasmissione di informazioni a terze parti nel caso l'utente fornisca un indirizzo e-mail errato.

8. Utenti di età inferiore a 16 anni

Lookout non raccoglie e non memorizza volutamente i Dati personali di minori di età inferiore a 16 anni, a meno che non facciano parte di un piano che comprende più dispositivi, sottoscritto da un genitore che ha acconsentito a tale raccolta e memorizzazione, come descritto nelle Condizioni del servizio di Lookout. Se si ritiene che il servizio sia utilizzato da un minore senza il consenso dei genitori, contattare Lookout all'indirizzo privacy@lookout.com.

9. Trasferimenti internazionali di dati

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 Lookout 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.

10. Termini aggiuntivi per i residenti in California

a. Informazioni personali

Ai sensi del California Consumer Privacy Act ("CCPA"), modificato dal California Privacy Rights Act, segue un elenco delle categorie di informazioni personali (intese secondo la definizione data dal CCPA) che raccogliamo (mediante l'app Personal o in altro modo), insieme alle categorie di fonti da cui abbiamo raccolto le informazioni, lo scopo commerciale per cui abbiamo raccolto le informazioni e le categorie di terzi con cui condividiamo le informazioni personali. Le informazioni presentate nella seguente tabella si riferiscono agli ultimi 12 mesi.

Categorie di informazioni personali	Categorie di fonti	Scopo commerciale	Categorie di entità a cui vendiamo, riveliamo o con cui condividiamo le informazioni personali per uno scopo commerciale
Dati identificativi, inclusi indirizzo e-mail, indirizzo IP, SSID del wi-fi e dati identificativi di altri dispositivi	Consumatore	Offrire un servizio, migliorare il servizio, assistenza clienti, analisi	Fornitori di analisi dei dati, fornitori di servizi e collaboratori esterni
*Dati identificativi per la protezione in caso di furto, inclusi codice fiscale, numero di patente di guida, carta di credito e numeri di conto corrente	Consumatore	Fornire servizi	Fornitori di servizi e collaboratori esterni
Dati di geolocalizzazione	Consumatore	Fornire servizi	Fornitori di servizi e collaboratori esterni
Informazioni relative alle interazioni di un consumatore con siti Web o applicazioni	Consumatore	Fornire servizi	Fornitori di servizi e collaboratori esterni

*Tutti i dati identificativi per la protezione dai furti vengono inseriti direttamente dal consumatore, conservati da un fornitore di servizi esterno di Lookout, CSID (che ora fa parte di Experian), e usati esclusivamente agli scopi previsti per l'erogazione dei servizi.

b. Diritti dell'utente

Ai sensi del CCPA e con riserva di eccezioni, i consumatori della California (intesi secondo la definizione data dal CCPA) dispongono dei seguenti diritti:

i. **Accesso.** L'utente ha il diritto di richiedere che Lookout riveli e fornisca le categorie di informazioni personali raccolte che lo riguardano, o informazioni personali specifiche raccolte dall'azienda in merito all'utente.

ii. **Cancellazione.** L'utente ha il diritto di richiedere la cancellazione delle informazioni personali in alcuni casi, con specifiche eccezioni previste dalla legge.

iii. **Correzione.** L'utente ha il diritto di correggere o rettificare le informazioni personali che conserviamo in archivio che lo riguardano.

iv. **Non discriminazione.** L'utente ha il diritto di non subire discriminazioni, incluso a titolo esemplificativo ma non esaustivo il diritto di non vedersi addebitati prezzi diversi per i servizi o vedersi negato l'accesso ai servizi in base alla sua decisione di esercitare i propri diritti enunciati in questa sezione. Ci impegniamo a non discriminare gli utenti per l'esercizio dei propri diritti previsti dal CCPA.

v. **Rifiuto esplicito.** Lookout non vende e non condivide le informazioni personali degli utenti dell'app Personal, quindi questo diritto non è applicabile all'utente.

vi. **Limitazione dell'utilizzo delle informazioni personali riservate.** Lookout non elabora le "Informazioni personale riservate" (intese secondo la definizione data dal CCPA) per nessuno scopo oltre a quelli consentiti nella sezione 7027(m) delle disposizioni del CCPA; pertanto, questo diritto non è applicabile all'utente.

L'utente può esercitare i propri diritti di accesso alle informazioni o di cancellazione delle informazioni in due modi: (1) completando il modulo Web accessibile alla pagina https://personal.support.lookout.com oppure (2) inviando una richiesta a Privacy@Lookout.com. Come indicato in precedenza nella sezione 5(a), per proteggere la privacy e la sicurezza dell'utente, è richiesto l'accesso al proprio account con nome utente e password al fine di verificarne l'identità prima di consentire l'accesso o di permettere di cancellare le informazioni personali. Se non possiamo verificare l'identità dell'utente, non riveleremo informazioni personali specifiche in risposta a una richiesta di accesso e rifiuteremo la richiesta di cancellare le informazioni personali a seguito di una richiesta di cancellazione. In caso di richiesta di cancellazione delle informazioni, Lookout applicherà un processo articolato in due passaggi, in cui prima l'utente dovrà inviare chiaramente la richiesta e in secondo luogo dovrà confermare separatamente l'intenzione di cancellare le informazioni personali. I consumatori della California possono incaricare un agente autorizzato di presentare richiesta di accesso o di cancellazione per loro conto, a condizione che l'agente autorizzato disponga dell'autorizzazione scritta e che l'utente possa verificare la propria identità direttamente con Lookout.

11. Termini aggiuntivi per i residenti dello Spazio economico europeo ("SEE")

a. Basi legali per il trattamento delle informazioni

Lookout è il responsabile del trattamento dei Dati personali (intesi secondo la definizione data dal Regolamento generale sulla protezione dei dati, "GDPR") dei visitatori provenienti dal SEE. La base legale per la raccolta e l'utilizzo dei dati personali degli utenti come indicato nella presente Informativa dipenderà dai Dati personali interessati e dal contesto specifico in cui sono raccolti. Tuttavia, Lookout raccogli i Dati personali degli utenti soltanto nei casi in cui: (a) è necessario utilizzare i Dati personali dell'utente per adempiere agli obblighi di un contratto con esso stipulato (ad esempio per ottemperare alle Condizioni del servizio, che l'utente accetta scaricando e utilizzando le app Lookout); oppure (b) l'utilizzo dei Dati personali dell'utente è giustificato da interessi legittimi di Lookout o di altri (ad esempio, per garantire la sicurezza dei servizi Lookout, per gestire e commercializzare i servizi Lookout, per garantire la sicurezza dell'ambiente di lavoro per il personale Lookout e per altri, per effettuare e ricevere pagamenti, per prevenire le frodi e per conoscere il cliente al quale vengono forniti i servizi Lookout); oppure (c) ha ottenuto il consenso dell'utente (ad esempio per determinate attività di marketing). Per uniformarsi alla legge applicabile può essere necessario trattare alcuni dati.

b. Privacy Shield

Lookout è una società autocertificata presso il Dipartimento del commercio statunitense come aderente al 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 un elenco delle entità che attualmente dispongono di certificazione come aderenti al Privacy Shield, visitare il sito http://www.privacyshield.gov.

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.

Con riferimento alle informazioni personali ricevute o trasferite ai sensi del Privacy Shield, Lookout è soggetta al potere esecutivo della Commissione federale per il commercio statunitense (Federal Trade Commission). In determinate situazioni, potrebbe essere chiesto a Lookout di divulgare informazioni personali in seguito a richieste legittime da parte delle autorità pubbliche, anche per soddisfare requisiti di sicurezza nazionale o di applicazione della legge.

Gli utenti che non sono soddisfatti della gestione delle problematiche relative alle procedure di Lookout in materia di privacy e all'elaborazione dei dati ai sensi del Privacy Shield, 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. Gli utenti 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).

Lookout è a conoscenza del fatto che la Corte di Giustizia dell'Unione Europea (CGUE) ha invalidato il Privacy Shield come certificazione di conformità alla legge sulla privacy dell'UE. Lookout ha sempre adempito ai propri obblighi in maniera indipendente, mediante informative sulla privacy con partner, clienti e utenti del nostro sito Web. Lookout si impegna a continuare a rispettare i requisiti applicabili per la tutela dei dati personali, in base alle disposizioni della legge vigente, delle norme e di altre autorità governative. Lookout si è impegnata inoltre a collaborare con il panel stabilito dalle autorità di protezione dei dati dell'UE e con l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) della Svizzera in merito ai reclami irrisolti del Privacy Shield inerenti i dati trasferiti dall'UE alla Svizzera. Lookout continuerà a seguire gli sviluppi relativi al quadro normativo sulla privacy dei dati UE-US e a garantire la conformità del trattamento dei dati personali alle leggi applicabili.

12. Diritti dei titolari dei dati

I residenti del Regno Unito, dello Spazio Economico Europeo o di altre giurisdizioni con leggi in vigore sulla protezione dei dati (ad esempio Virginia, Colorado, Connecticut e Utah) possono disporre di alcuni diritti relativi ai dati personali. Tali diritti possono essere soggetti a determinate esenzioni. Questi diritti includono:

i. **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.

ii. **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;

iii. **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); Oltre ai diritti concessi ai sensi della sezione riportata in precedenza, dal titolo "Possibilità di accedere e aggiornare le impostazioni sulla privacy", sono disponibili ulteriori informazioni inviando una richiesta a Lookout all'indirizzo privacy@lookout.com;

iv. **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;

v. **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;

vi. **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;

vii. **Revoca del consenso.** Il trattamento dei Dati personali da parte di Lookout si basa sul consenso degli utenti, i quali hanno il diritto di revocare tale consenso in qualsiasi momento.

viii. **Presentazione di un reclamo a un'autorità di controllo dei dati.** A seconda della giurisdizione, l'utente potrebbe avere il diritto di presentare un reclamo all'autorità locale di controllo dei dati se ritiene che stiamo violando la legge sulla protezione dei dati.

Gli utenti che desiderano esercitare tali diritti devono contattare Lookout all'indirizzo privacy@lookout.com. L'Azienda si impegna a rispondere alle richieste nel periodo previsto dalla legge in vigore. Prima di evadere la richiesta, potremmo richiedere all'utente di verificare la propria identità. L'identità verrà verificata mediante invio di un'e-mail all'indirizzo e-mail associato all'account dell'utente oppure mediante richiesta di ulteriori informazioni relative all'account. L'utente può anche incaricare un agente autorizzato di presentare richiesta per proprio conto (ma potremo comunque richiedere la verifica dell'identità).

13. Come contattare Lookout per sottoporre richieste o domande

Per contattare il Responsabile della protezione dei dati è possibile utilizzare l'indirizzo e-mail privacy@lookout.com, o l'indirizzo postale di Lookout, Inc., Att.: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA (USA) 02108, sottoponendo domande o commenti sulla presente Informativa. I residenti del SEE possono anche inviare domande all'attenzione di Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem, Paesi Bassi.