Lookout Persoonlijk privacybeleid

Creatiedatum: 15/11/2016
Revisiedatum: 22/05/2018
Status: Goedgekeurd

Revisiegeschiedenis

Lookout, Inc. beheert dit document en daarom wordt het afdrukken van het materiaal gezien als een 'referentiekopie'. Gebruikers hebben de verantwoordelijkheid te zorgen dat ze de nieuwste versie hebben. Als een deel van dit beleid moet worden bijgewerkt, dan wordt het hele document opnieuw uitgegeven.

Uitgave	Datum	Beschrijving	Verzonden door
1.0	22/09/2016	Initieel concept:	Marcelo Guerra
2.0	26/09/2017	Bijgewerkt	Joseph Leung
3.0	01/04/2018	Update om productwijzigingen vast te leggen en updates in regelgeving te beschrijven. Gegevens documentgeschiedenis verplaatst naar einde van document.	Kimberly Snow

Ingangsdatum: 25 mei 2018

Dit document is ons privacybeleid, waarin wordt beschreven welke informatie we van u verzamelen en hoe we deze gebruiken. Het is belangrijk dat u het privacybeleid leest naast de Servicevoorwaarden van Lookout (beschikbaar op www.lookout.com/legal/terms) omdat beide documenten van toepassing zijn op uw gebruik van de Lookout Personal App. Onze privacybeleid is van toepassing op onze websites en mobiele websites inclusief op www.lookout.com, onze Lookout Personal App, en alle andere diensten van Lookout die geleverd worden als onderdeel van de Lookout Personal App (zoals die voorwaarde is gedefinieerd in onze Servicevoorwaarden).

Het privacybeleid van het Lookout Enterprise Mobile Endpoint Security-product is beschreven in de Lookout Ondernemingsprivacyverklaring.

In deze privacyverklaring worden de verzameling en het gebruik van persoonsgegevens (PG) beschreven. Persoonsgegevens (PG) die van u worden verzameld omvatten onder andere gegevenselementen als uw naam, e-mailadres, telefoonnummer en/of de unieke identificator van uw mobiele apparaat. De term persoonsgegevens omvat ook persoonlijk identificeerbare informatie en persoonsgegevens als gedefinieerd in de AVG Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) ('AVG').

Lookout behoudt zich het recht voor deze privacyverklaring aan te passen aan wijzigingen in de wet, onze gegevensverzamelings- en gebruikspraktijken, de kenmerken van onze diensten of technologische ontwikkelingen. Controleer dit document of de internetpagina's op Lookout.com regelmatig op wijzigingen. Door gebruik te blijven maken van onze diensten, gaat u akkoord met deze wijzigingen en komt u overeen te zijn gebonden aan het bijgewerkte beleid. Neemt u contact met ons op via privacy@lookout.com als u vragen hebt over dit privacybeleid. U kunt dit privacybeleid inzien vanaf het aanmeldscherm van de mobiele applicatie van Lookout, vanuit de instellingen in de Lookout Personal App en vanaf de website van het bedrijf.

Producten die worden aangeboden in de Lookout Personal App

Lookout biedt meerdere lagen in de Lookout Personal App. Ieder laag biedt extra toegang tot beveiligingsfuncties van Lookout. De informatie die nodig is om deze diensten te bieden, kan verschillen en is vermeld in dit document, zodat u weet welke informatie wij rechtstreeks van u en van uw apparaat verzamelen en hoe we deze informatie gebruiken. Informatie betreffende productfuncties voor de Lookout Personal App voor iOS- en Android-apparaten vindt u hier https://www.lookout.com/products/personal/ios en https://www.lookout.com/products/personal/android.

1. We verzamelen informatie van u om u te voorzien van Lookout-diensten

Als we uw informatie verzamelen, slaan we deze op en koppelen we deze aan uw account, tenzij anders vermeld. We nemen uw privacy hoog op en we gebruiken en geven uw informatie alleen vrij als beschreven in het privacybeleid.

Een aantal van onze producten zijn standalone producten, en verzamelen slechts beperkte informatie of helemaal geen informatie. De beschikbaarheid van functies verschilt per product en per land. Daarom zijn niet alle paragrafen van dit privacybeleid van toepassing op deze producten.

Let erop dat we bepaalde soorten informatie nodig hebben voor het leveren van de Lookout-diensten aan u. Als u dergelijke informatie niet aan ons verschaft, of als u ons vraagt deze te verwijderen, kan het zijn dat u niet langer toegang hebt tot de Lookout-diensten.

Let erop dat ons doel voor het verzamelen van applicatiegegevens en beveiligingsscangegevens het bieden van bescherming en het beveiligen van uw gegevens is. Dit is ook om onze Lookout-diensten te optimaliseren en verbeteren.

Lookout verzamelt gegevens over uw apparaat, waaronder valt het merk, model, type besturingssysteem en revisie, alsmede welke applicaties zijn geïnstalleerd. Deze gegevens worden gede-identificeerd en gecombineerd met gede-identificeerde gegevens van andere klanten om de populariteit van apparaten in applicaties per regio te genereren. Deze gegevens blijven gede-identificeerd om te zorgen voor de privacy van persoonsgegevens. Door klantgegevens te combineren op veilige en vertrouwelijke wijze, krijgt Lookout meer inzicht in de huidige beveiligingsdreigingen. We kunnen zo ook de functies en diensten van Lookout verbeteren. We kunnen ook openbaar rapporten delen die voortvloeien uit de analyse van deze gegevens, om anderen te helpen inzicht te krijgen in mobiele dreigingen en in specifiek mobiel applicatiegedrag.

2. Informatie die Lookout verzamelt voor de Lookout Basic Personal App

a. Registratie-informatie

Om een account te kunnen maken, moet u een e-mailadres en wachtwoord opgeven.

b. Apparaatinformatie

Als u Lookout-diensten gebruikt, leggen onze servers bepaalde informatie vast over uw mobiele apparaat. Onder deze informatie kan vallen een apparaatidentificator (bijv. IMEI, abonnee-identificatie (bijv. IMSI), apparaatnaam, mobiel telefoonnummer, apparaattype en -producent, type en versie besturingssysteem, draadloze provider/operator, netwerktype, land van herkomst, Internet Protocol (IP)-adres, en de data en tijden van uw verzoeken. We verzamelen ook informatie over de applicaties op uw apparaat om scans uit te voeren en kopieën van gescande applicatiebestanden te downloaden. Hieronder kan vallen het downloaden van een kopie van een deel van of volledige kopieën van applicatiebestanden op uw apparaat als we een applicatie ontdekken die we niet eerder hebben geanalyseerd. We kunnen ook informatie verzamelen over hoe applicaties zich gedragen op uw apparaat (bijv. of een applicatie tekstberichten verzendt tegen verhoogd tarief die op uw factuur in rekening worden gebracht) en de netwerkdiensten waarmee uw applicaties communiceren, om te bepalen of applicaties kwaadwillig zijn (bijv. of een applicatie communiceert met een server waarvan bekend is dat deze phishing-websites host). Iedere keer wanneer Lookout een scan uitvoert, kunnen we informatie verzamelen die beschrijft welke applicatiebestanden door de scan zijn geïdentificeerd als mogelijk ongewenst. Lookout biedt vervolgens aanbevolen keuzes voor herstel van die bestanden (bijv. verwijderen of negeren).

We gebruiken de hierboven beschreven informatie om onze diensten te bieden, en indien nodig ondersteuning. We voegen ook informatie samen over mobiele dreigingsanalyses. Informatie die in samengevoegde indeling wordt bewaard, wordt gede-identificeerd om te zorgen dat een individueel persoon niet kan worden geïdentificeerd.

Ga voor meer informatie over Lookout mobiele dreigingsinformatie naar https://www.lookout.com/why-lookout.

c. Locatie-informatie

Sommige functies die we aanbieden, werken beter als we uw mobiele apparaat kunnen lokaliseren. Met uw toestemming, die u geeft tijdens de initiële registratie, kan Lookout op twee manieren informatie verzamelen. We kunnen deze direct van uw mobiele apparaat ontvangen of, in sommige gevallen, kunnen we locatiegegevens ontvangen van een mobiele zendmast of wifihotspot-informatie. We kunnen gebruik maken

van derde serviceleveranciers om die informatie te vertalen naar bruikbare locatie-informatie. Om te voorkomen dat locatiegegevens worden gedeeld, gaat u naar de instellingen van uw mobiele apparaat en schakelt u locatiediensten uit.

d. URL's

Om de Safe Browsing-dienst te bieden, kunnen we de URL's die u ontvangt of bezoekt op uw telefoon verzenden aan een door Lookout of derde partij geleverde dienst om te bepalen of die URL's onveilig zijn (bijv. of de URL's phishing-aanvallen, malware of exploits bevatten). Als een URL die u wilt bezoeken onveilig blijkt, dan slaan we een dossier van de onveilige URL op. We gebruiken het dossier van de onveilige URL's die u bezoekt (1) om u een melding te sturen dat de URL die u probeert te bereiken onveilig is (bijv. wanneer u zich aanmeldt bij de Lookout-website of via e-mail) en (2) om ons product en gedragsanalyse te verbeteren. Als u niet wilt dat wij de onveilige URL's die u bezoekt, documenteren, dan kunt u Safe Browsing uitschakelen; alle andere functies van Lookout blijven dan gewoon functioneren.

3. Functies die worden aangeboden in de Lookout Personal App

a. Beveiliging

De beveiligingsfuncties van Lookout, die beschikbaar zijn op verschillende platformen, helpen bij het beschermen van uw apparaten tegen cyberveiligheidsdreigingen. De informatie die nodig is om deze functies te ondersteunen, wordt verzameld als u de Lookout App gebruikt. Details over deze informatie zijn vastgelegd in de sectie Apparaatinformatie van dit document.

De beveiligingsfuncties van Lookout, die per platform verschillen, bieden beveiliging via verschillende middelen, waaronder scannen naar kwaadwillende apps en bestanden en het detecteren van een verouderd besturingssysteem. U vindt meer informatie over de voorspellende beveiligingstechnologie van Lookout op www.lookout.com. Er kunnen periodiek automatische scans worden uitgevoerd van uw apparaat om informatie te verzamelen over de applicaties, het apparaat en de besturingssysteembestanden op uw apparaat. Lookout verzamelt de resultaten van scans die worden uitgevoerd door onze diensten en de recentste beveiligingsinstelling van het apparaat. Daarnaast worden regelmatig updates van dreigingsdefinities uitgevoerd. Deze activiteiten helpen bij het beschermen van uw mobiele eindpunt door de Lookout App dreigingen op uw mobiele apparaat te laten detecteren en aanpakken. Deze functie kan worden uitgeschakeld via de instellingen van de Lookout App.

b. Verloren apparaat

De diefstalpreventiefuncties van Lookout omvatten de mogelijkheid Missing Device, zoals de functie Locate

and Scream, waarmee u uw apparaat op afstand vanaf uw persoonlijke account op lookout.com kunt zoeken en vergrendelen. Met de functie Signal Flare kunt u uw telefoon zoeken in de buurt van de laatst bekende locatie als u hem verliest en de batterij leeg is. Als u Signal Flare hebt ingeschakeld, verzamelt deze functie locatie-informatie en stuurt deze terug naar Lookout als de batterij bijna leeg is. We slaan de locatie van de telefoon op Lookout.com op wanneer we de melding ontvangen dat de batterij bijna leeg is. Deze functie kan worden uitgeschakeld via de instellingen van de Lookout App.

Als u de functies voor Missing Device inschakelt, stuurt uw browser locatie-informatie naar externe leveranciers van kaarten (bijv. Google Maps) om een kaart weer te geven van de locatie op uw persoonlijke account op lookout.com. Als u deze functie hebt geactiveerd, traceren we de locatie van het apparaat gedurende een aantal minuten om een nauwkeurige locatie van uw apparaat aan u door te kunnen geven. Deze informatie wordt opgeslagen in uw accountgeschiedenis en kan door u op ieder moment worden verwijderd uit uw accountinstellingen. Als u deze informatie verwijdert of uw account deactiveert, de-identificeert Lookout deze gegevens, zodat ze niet langer zijn gekoppeld aan uw persoonsgegevens.

c. Back-up (contacten)

Met Lookout Backup kunnen gebruikers een back-up maken van hun contacten. Deze informatie wordt verzonden naar servers door middel van een versleuteld protocol en opgeslagen in de Lookout Cloud. De informatie kan worden geopend of verwijderd door u aan te melden op uw account op Lookout.com. Deze functie kan worden uitgeschakeld via de instellingen van de Lookout App.

d. Ondersteuning van meerdere apparaten

Multiple Device Support koppelt meerdere apparaten aan één hoofdaccount waarmee het apparaat van de eigenaar van de hoofdaccount wordt beheerd, evenals bepaalde functies van apparaten die zijn gekoppeld aan het hoofdaccount. Eigenaars van een hoofdaccount hebben de controle over een aantal functies van de extra apparaten. In een account met meerdere apparaten kan een gebruiker bijvoorbeeld back-upgegevens zoeken of gebruiken op een apparaat dat is ingeschreven onder hetzelfde account.

4. Informatie die Lookout verzamelt voor onze Premium Services in de Personal App

a. Informatie die wordt verzameld bij het opwaarderen naar Premium Service

Lookout verzamelt dezelfde informatie als vermeld in de Lookout Basic Personal App; registratie-informatie, apparaatinformatie, locatie-informatie (indien nodig). Naast deze informatie verzamelt Lookout ook betaalinformatie zodat u premiumfuncties kunt gebruiken.

b. Betaalinformatie

Als u rechtstreeks bij ons een abonnement afneemt voor Premium of Premium Plus Lookout-diensten gebruiken we een derde betalingsverwerker voor het verzamelen van uw creditcardgegevens, inclusief uw creditcardnummer, vervaldatum, veiligheidscode en andere toepasbare facturatie-informatie. Onze derde verkoper gebruikt deze informatie om u te factureren voor de diensten. Lookout heeft informatie betreffende uw Premium- en/of Premium Plus-account. Onder deze informatie valt het bedrag dat u hebt betaald en de betaalmethode. We ontvangen uw creditcard- of bankgegevens niet. Deze informatie blijft bij de derde betalingsverwerker.

Als u de Lookout App aanschaft via een App Store of via het dataplan van uw serviceprovider, worden uw betaalgegevens beheerd door die App Store of provider. De betaling gaat niet naar Lookout. Uw betaling kan op verschillende manieren worden verwerkt. Lookout heeft contractovereenkomsten met onze Partners om te zorgen dat de Lookout mobiele app werkt zoals u verwacht. Om onze diensten aan u te leveren, stuurt de App Store Lookout een bevestiging van uw aankoop. Serviceproviders kunnen uw telefoonnummer, abonnement-ID, SKU en andere niet-financiële informatie delen. De App Store en uw serviceprovider delen geen creditcard- of factuurinformatie. Zie voor aanvullende informatie het beleid en de procedures voor betalingsverwerking van de App Store of serviceprovider.

c. Gegevensverzameling diefstalmelding

Als Theft Alerts is ingeschakeld, wordt een foto genomen. De foto en de locatiegegevens (GPS-locatie) worden kort opgeslagen op onze servers, zodat we u een e-mail kunnen sturen met de foto en een kaart van de locatie van uw apparaat. De foto wordt dan van onze server verwijderd. We sturen de e-mail naar het adres dat is gekoppeld aan uw account, dus onthoud dat u uw e-mailadres up-to-date moet houden in uw accountinstellingen. We gebruiken informatie over activiteiten van Theft Alert op uw apparaat om onze producten te bestuderen, optimaliseren en problemen op te lossen.

d. Veilig surfen

Safe Browsing is een functie die is ontwikkeld voor het identificeren van en waarschuwen voor onveilige URL's, zodat u ervoor kunt kiezen deze niet te laden. Safe Browsing is voor u beschikbaar als u de app hebt toegestaan op een lokaal VPN te draaien. Aan de hand van het VPN scannen de functies van Safe Browsing URL's die op uw apparaat worden geopend via browsers en apps. Bezochte URL's worden geanonimiseerd en verzonden naar de Lookout Cloud om beveiligingsscans uit te voeren. URL-paden zijn de enige gegevens met betrekking tot uw surfactiviteiten die worden verzonden aan Lookout. Lookout verzamelt geen surfgeschiedenis of andere persoonlijke informatie.

5. Functies geleverd bij Lookout Premium Service

Naast bovenstaand beschreven basisfuncties, krijgen Lookout Premium-klanten toegang tot nieuwe functies en functieverbeteringen.

a. Verloren apparaat

Premium-abonnees van Lookout ontvangen extra mogelijkheden binnen de functie Missing Device. De mogelijkheid het apparaat op afstand te vergrendelen en wissen wordt geboden vanaf uw persoonlijke account op lookout.com.

b. Diefstalmeldingen

Theft Alerts is een premium functie binnen Theft Protection. Met Theft Alerts kunt u uw telefoon zoeken als die kwijt is. Als deze functies zijn ingeschakeld, wordt bij geselecteerde gebeurtenissen een e-mail aan u verzonden (bijv. vliegtuigmodus ingeschakeld) met de locatie van uw apparaat. Bij Android-apparaten bevat de e-mail een foto van de persoon die hem zou kunnen hebben gestolen, gemaakt met de camera van uw apparaat en locatiefuncties om u te helpen achterhalen waar uw apparaat zou kunnen zijn (en wie het kan hebben) in het geval dat uw apparaat is verloren of gestolen.

U kunt de locatie van uw apparaat zien door u aan te melden bij uw account op lookout.com. Deze functies gebruiken de locatiegegevens van uw apparaat, e-mail en telefoonnummer die u aan Lookout hebt vermeld vanaf het apparaat en helpen u bij het terugvinden van uw telefoon wanneer u hem verloren hebt.

c. Back-up (Oproepoverzichten en foto's)

De back-up van oproepoverzichten en foto's wordt ondersteund voor Premium-abonnees. U kunt uw foto's dan openen via uw persoonlijke account op Lookout.com. Uw foto's en opgeslagen gegevens kunnen op ieder moment van uw Lookout-account worden verwijderd.

d. Veilig surfen

Safe Browsing is een functie die is ontwikkeld voor het identificeren van en waarschuwen voor onveilige URL's, zodat u ervoor kunt kiezen deze niet te laden. Safe Browsing is voor u beschikbaar als u de app hebt toegestaan op een lokaal VPN te draaien. Aan de hand van het VPN scannen de functies van Safe Browsing URL's die op uw apparaat worden geopend via browsers en apps. Bezochte URL's worden geanonimiseerd en verzonden naar de Lookout Cloud om beveiligingsscans uit te voeren. URL-paden zijn de enige gegevens met betrekking tot uw surfactiviteiten die worden verzonden aan Lookout. Lookout verzamelt geen surfgeschiedenis of andere persoonlijke informatie.

e. Veilige wifi

Met Safe Wi-Fi analyseert Lookout uw wifi-verbinding op ongewone activiteit die erop duidt dat het netwerk onveilig is of wordt aangevallen. U wordt dan gewaarschuwd. Safe Wi-Fi helpt voorkomen dat aanvallers uw persoonsgegevens op uw mobiele eindpunt kunnen inzien.

f. Overtredingsrapport (alleen beschikbaar in het Engels)

Met Breach Report kan Lookout u op de hoogte brengen van relevante overtredingen, met duidelijke en eenvoudige acties die u kunt ondernemen om uzelf te beschermen. U kunt meldingen aanpassen aan specifieke bedrijven of industrieën, en u ontvangt ook aanbevelingen over welke acties u moet ondernemen om uw gegevens en identiteit te beschermen.

g. Functies uitschakelen

Als u daarvoor kiest, kunt u functies uitschakelen met behulp van de Lookout-instellingen. Neem bij problemen en vragen contact op met support@lookout.com.

6. Informatie die wordt verzameld met Lookout Premium Plus (Alleen VS)

De informatie die we verzamelen is afhankelijk van de soorten identiteitsbeschermingsproducten van Premium Plus waarvoor u zich inschrijft. Deze informatie is nodig om uw identiteit te controleren, u te voorzien van de gevraagde identiteitsbeschermingsdiensten en u de overeengekomen tarieven in rekening te brengen. Het is nodig uw informatie te communiceren aan derde partijen (zoals identificatieverificatiebedrijven, consumentenrapportagebureaus, kredietcontrolebureaus, betalingscontrolebedrijven, wetshandhavingsinstellingen en anderen) om u die diensten te kunnen leveren. We kunnen deze informatie verstrekken aan onze derde serviceleveranciers die ons helpen bij het voorzien in identiteitsbeschermingsdiensten, of deze serviceleveranciers toestemming geven bepaalde informatie rechtstreeks bij u te verzamelen. Deze serviceleveranciers kunnen op hun beurt uw gegevens verstrekken aan derde partijen met als doel u te voorzien van de gevraagde diensten. Wij en/of onze serviceleveranciers kunnen u ook voorzien van bewaking en meldingen en informatie en rapporten over u verkrijgen (of over anderen die u hebt ingeschreven) om de identiteitsbeschermingsdiensten te bieden, inclusief adresgeschiedenis, naam, alias en andere rapporten. We verplichten onze serviceleveranciers de gegevens die van u worden verzameld alleen te gebruiken voor doeleinden van het bieden van diensten via Lookout App Premium Plus. Als u opwaardeert naar een Premium Plus-abonnement met daarin identiteitsdiefstalverzekering, gebruiken we uw informatie om u te voorzien van hulp en toepasselijke verzekeringsdekking als u identiteit wordt aangetast.

Als u zich inschrijft voor Premium Plus, kan de Lookout App uw contactinformatie vragen (zoals naam, adres, telefoonnummer en e-mailadres); privé-informatie (zoals rijbewijsnummer, burgerservicenummer, paspoortnummer of andere identificatienummers); financiële informatie (zoals bankrekening, nummers van betaalpas en creditcard); medisch verzekeringsnummer en andere persoonlijke gegevens over u (of andere mensen die u inschrijft voor de dienst). Ga voor aanvullende informatie of updates naar de Productparagraaf op Lookout.com.

7. Aangeboden functies bij Premium Plus (Alleen VS)

Naast de basisfuncties (Missing Device, Security en Backup) en premium diensten (Theft Alerts, Safe Wi-Fi, Breach Report, Photo Backup), kunnen Premium Plus-gebruikers gebruikmaken van Identity Protection, waaronder valt Identity Monitoring, Identity Insurance en Restoration.

1. Identiteitsbewaking

Door op te waarderen naar Premium Plus ontvangt u diensten die u helpen bij het beschermen van uw identiteit en persoonsgegevens.

a. Cyber-bewaking

Cyber Watch monitort het internet op uw privé-informatie en geeft meldingen en aanbevolen acties als uw persoonsgegevens openbaar zijn gemaakt.

b. Sociale media-bewaking

Social Media Watch controleert de privacy van uw persoonsgegevens op sociale netwerken en stuurt u meldingen over ongepaste posts.

c. Bewaking van burgerservicenummer

SSN Watch stuurt meldingen wanneer nieuwe namen en adressen worden gekoppeld aan uw burgerservicenummer.

2. Verzekering en herstel

Lookout helpt u de hoofdpijn en problemen op te lossen die gepaard gaan met het herstellen van uw identiteit als deze wordt gestolen.

a. Identiteitsdiefstalverzekering

Lookout Premium Plus biedt dekking van juridische kosten, inkomstenderving en andere kosten die zijn gekoppeld aan het herstellen van uw gestolen identiteit.

b. Hulp bij herstel

Lookout biedt 24/7 hulp van identiteitsherstelexperts die u kunnen helpen uw identiteit te herstellen als deze wordt gestolen.

c. Herstel verloren portemonnee

Lookout helpt u bij het blokkeren en vervangen van betaalpassen, ID's en andere inhoud van uw portemonnee als deze is gestolen of verloren.

8. Klantenservice mobiele operator voor KDDI-klanten

Als uw mobiele operator deelneemt aan ons Mobile Operator Customer Care-programma, kunt u uw mobiele operator bellen om uw telefoon of tablet te zoeken en vergrendelen als deze is gestolen of verloren.

Lookout heeft informatie over u en uw apparaat nodig om klantenservice te kunnen bieden. De Customer Care Web Application verzamelt uw telefoonnummer, indien beschikbaar, en informatie over het soort apparaat en besturingssysteem dat u gebruikt om te zorgen dat medewerkers van de klantenservice de externe functies op uw apparaat nauwkeurig kunnen identificeren en beheren.

Lookout gebruikt uw informatie om de medewerker van de klantenservice te informeren, zodat hij het verwachte niveau aan klantenservice kan bieden.

Met de Customer Care Application kunnen mobiele operators en hun klantenservicemedewerkers op uw verzoek externe functies op uw apparaat uitvoeren, waaronder:

- Het apparaat opsporen
- Het apparaat vergrendelen
- Het apparaat wissen
- Een hard alarm inschakelen (Scream)
- Een bericht verzenden aan het apparaat.

Medewerkers van de klantenservice mogen dergelijke functies alleen op uw verzoek uitvoeren en met uw voorafgaande toestemming.

Om de privacy van gebruikers te beschermen, waarschuwt Lookout u via het e-mailadres dat we van u hebben wanneer een medewerker van de klantenservice een van bovenstaande functies uitvoert. Medewerkers van de klantenservice hebben geen toegang tot of controle over gebruikersgegevens waarvan een back-up is gemaakt via de mobiele applicatie van Lookout.

9. Gegevensanalyse: hoe we de informatie gebruiken die we van uw Mobile Endpoint-apparaat verzamelen

We kunnen de resultaten van onze gegevensanalyses gebruiken om u relevante inhoud te sturen, nieuwe functies of producten en/of diensten voor te stellen die uw ervaring met de Lookout-diensten kunnen verbeteren. We koppelen de informatie die we in de analysesoftware opslaan niet aan persoonsgegevens die u verzendt via de mobiele app. Daarnaast wordt informatie die in samengevoegde indeling wordt bewaard, ook gede-identificeerd om te zorgen dat een individueel persoon niet kan worden geïdentificeerd.

Naast het gebruiken van de informatie die u aan ons verzendt en de informatie die we verzamelen van uw mobiele eindpuntapparaat om de Lookout-diensten te leveren, gebruiken we ook de informatie die wordt verzameld van uw apparaat om gegevensanalyses uit te voeren. Deze analyses bieden belangrijke informatie waarmee we de functies en bruikbaarheid van onze producten kunnen verbeteren. We analyseren informatie zoals hoe vaak u de Lookout-applicatie gebruikt op uw mobiele eindpuntapparaat, de gebeurtenissen die voorvallen binnen de Lookout-applicatie op uw mobiele eindpuntapparaat en waar de Lookout-applicatie is gedownload op uw mobiele eindpuntapparaat. We gebruiken deze informatie ook in samengevoegde vorm om analyses uit te voeren op bestaande en nieuwe mobiele dreigingen.

10. Uw gebruik van de website en mobiele website van Lookout en informatie die we verzamelen

Als u de website van Lookout gebruikt vanaf uw computer of mobiele eindpunt, kan Lookout vrijwillige informatie van u verzamelen om uw gebruikerservaring te verbeteren. Lookout kan ook analysediensten op de achtergrond gebruiken om te meten hoe mensen onze website en e-mails gebruiken, zodat we onze producten en diensten kunnen verbeteren en u relevantere inhoud kunnen bieden. Analysediensten op onze website en mobiele website kunnen werken door het inbouwen van onzichtbare afbeeldingen die zijn gekoppeld aan unieke identifiers op onze site, door het gebruik van cookies of andere lokaal op het apparaat opgeslagen bestanden of door het gebruik van web beacons, web bugs, clear gifs en vergelijkbare traceertechnologieën.

a. Inhoud en promoties

We kunnen u vragen om uw e-mailadres en andere contactinformatie tijdens uw bezoek aan onze websites om

u toegang te bieden tot diverse Lookout-inhoud, zoals whitepapers, video's en andere onderzoeksmaterialen. We kunnen u ook vragen deel te nemen aan onderzoeken, wedstrijden, promoties en verlotingen. We kunnen uw feedback vragen omtrent uw ervaring met de producten en diensten van Lookout. Uw contactgegevens worden gebruikt om u te voorzien van aanvullende informatie over producten en diensten van Lookout en onze zakenpartners. U kunt ervoor kiezen dergelijke marketingcommunicatie niet te ontvangen door op de koppeling voor uitschrijven te klikken in onze e-mails, zoals verder hieronder beschreven.

b. Sociale media-functies

Op onze website staan sociale media-functies ('functies'), zoals de knop 'like' of interactieve mini-programma's die op onze site draaien. Als u deze functies gebruikt, verzamelen ze uw IP-adres, welke pagina u bezoekt op onze site en plaatsen ze een cookie om te zorgen dat de functies correct werken. De functies kunnen gehost worden door een derde partij of direct op de site worden gehost. Uw interacties met deze functies van derde partijen vallen onder het privacybeleid van het bedrijf dat de functie aanbiedt, niet onder het privacybeleid van Lookout.

11. Lookout websitecookiebeleid

1. Soorten cookies

Net als vele andere online dienstverleners, gebruiken we cookies en andere middelen om informatie over u en uw gebruik van onze producten en diensten te verzamelen en analyseren. We gebruiken deze technologieën om relevante inhoud te bieden over de producten en diensten van Lookout. Cookies zijn kleine gegevensbestanden die we op uw computer of apparaat opslaan. Voor meer informatie zie aboutcookies.org.

2. Hoe we cookies gebruiken

We gebruiken 'sessiecookies' om u aangemeld te houden als u onze diensten gebruikt, om meer inzicht te krijgen in uw interactie met onze diensten en om samengevoegde gebruiks- en webverkeerinformatie over onze diensten te controleren. Sessiecookies verdwijnen als u zich afmeldt en uw browser sluit. We gebruiken ook 'permanente cookies' om u te herkennen als u onze diensten opnieuw gebruikt. Permanente cookies kunnen gedurende een langere tijd dan een sessiecookie op uw computer blijven staan. We gebruiken ook 'analysecookies'. Hiermee kunnen we het aantal bezoekers herkennen en tellen, zien hoe bezoekers op onze pagina's bewegen en hoe zij deze gebruiken. Zo kunnen we de manier verbeteren waarop onze website werkt, bijvoorbeeld door te zorgen dat gebruikers eenvoudig vinden wat ze zoeken. Ten slotte kunnen we andere standaardtechnologieën gebruiken, zoals web beacons, web bugs, clear gifs en lokale opslag, voor het analyseren, verzamelen en samenvoegen van gegevens over uw gebruik van onze producten en diensten.

3. Cookies van derde partijen

Wij zijn van mening dat het belangrijk is dat u precies weet welke cookies van derde partijen we gebruiken op onze website en diensten. Hieronder staat een lijst van de cookies van derde partijen die we gebruiken, die na verloop van tijd persoonsgegevens over uw online activiteiten en via verschillende websites of online diensten van derde partijen kunnen verzamelen. We ontwikkelen en verbeteren onze diensten en we kunnen andere derde partijen gebruiken. We werken deze lijst dienovereenkomstig bij. We hebben ook een koppeling opgenomen naar het privacybeleid dat van toepassing is op de cookie van de derde partij.

- Google Analytics: Met deze cookies kunnen we zien hoe u onze website en mobiele applicatie gebruikt, zodat we uw ervaring kunnen verbeteren. We raden u aan het Google Privacybeleid te lezen. Als u niet wilt dat er gegevens worden gerapporteerd door Google, dan staat Google u toe zich uit te schrijven door de Google Analytics Opt-out Browser Add-on te installeren.
- Google AdWords: Met deze cookies kunnen onze verkopers reclames aanbieden op basis van uw vorige bezoeken aan onze site en voor remarketingdoeleinden. Google kan dit cookie en ander traceertechnologie gebruiken om u reclames te tonen op het internet. Google geeft u de mogelijkheid u uit te schrijven voor Google's gebruik van deze cookies door middel van Google's Reclame-instellingen.
- Marketo: Met deze cookies kunnen we uw bezoeken aan onze website traceren en kunnen we een aantrekkelijke marketingervaring voor u creëren. We gebruiken Marketo-cookies ook om inzicht te krijgen in uw interactie met de e-mails die we u sturen en om te zorgen dat we u relevante informatie sturen. Marketo-cookies vertellen ons bijvoorbeeld of onze e-mails zijn gelezen en op welke koppelingen is geklikt. U kunt het Marketo privacybeleid hier lezen.
- Sociale media-functies: Op onze website staan sociale media-functies, zoals de knop Aanraden of interactieve mini-programma's die op onze site draaien. Als u deze functies gebruikt, verzamelen ze uw IP-adres, welke pagina u bezoekt op onze site en plaatsen ze een cookie om te zorgen dat de functie correct werkt. De functies kunnen gehost worden door een derde partij of direct op de site worden gehost. Uw interacties met deze functies vallen onder het privacybeleid van het bedrijf dat de functie aanbiedt, niet onder het privacybeleid van Lookout.
- Mixpanel, Braze en mParticle: Met deze cookies kunnen we gegevens analyseren en samenvoegen van uw gebruik van onze mobiele applicatie. We raden u aan het MixPanel privacybeleid, Braze privacybeleid en mParticle privacybeleid te lezen.

12. Rechtsgrond voor het gebruik van uw informatie

De rechtsgrond voor het gebruik van uw informatie als vermeld in dit privacybeleid is als volgt: (a) Gebruik van uw persoonsgegevens is noodzakelijk om onze verplichtingen uit te voeren onder een contract met u (bijvoorbeeld om te voldoen aan de Servicevoorwaarden die u accepteert door onze apps te downloaden en gebruiken); of (b) Waar gebruik van uw informatie niet nodig is voor het uitvoeren van een contract, maar gebruik van uw informatie nodig is voor onze rechtmatige belangen of de rechtmatige belangen van anderen (bijvoorbeeld om te zorgen voor de beveiliging van de Lookout-diensten, het uitvoeren van de Lookout-diensten, zorgen voor veilige omgevingen voor ons personeel en anderen, het doen en ontvangen van betalingen, het voorkomen van fraude en het kennen van de klant aan wie we de Lookout-diensten leveren). Sommige verwerkingsactiviteiten worden uitgevoerd om te voldoen aan toepasselijke wetgeving.

In sommige gevallen (zoals voor sommige van onze marketingactiviteiten), kunnen we uw persoonsgegevens verwerken op basis van toestemming.

Naast het specifieke gebruik als hierboven beschreven, gebruiken we uw informatie ook op de volgende manier:

a. We gebruiken uw informatie voor het bieden, verbeteren en promoten van onze diensten

We gebruiken uw informatie om u te voorzien van een betere dienstverlening, om onze producten en diensten te verbeteren, om onze diensten te promoten en nieuwe diensten te ontwikkelen. Bijvoorbeeld:

- Als u een onderzoek invult of Lookout mailt voor hulp, kunnen we die informatie bewaren om u te voorzien van hulp en om onze diensten te verbeteren.
- Waar beschikbaar kan Lookout informatie van klantenapparaten gebruiken om u te laten weten dat u uw besturingssysteem moet bijwerken.
- We kunnen sms-berichten naar uw telefoon verzenden om te communiceren met uw apparaat.
- We kunnen uw e-mailadres of mobiel nummer gebruiken om aan privacy of beveiliging gerelateerde meldingen te sturen en u te informeren over grote serviceveranderingen van Lookout.
- We kunnen uw e-mailadres of mobiel telefoonnummer gebruiken om te communiceren over productaankondigingen en speciale aanbiedingen van Lookout of onze zakenpartners, of om deelname te administreren aan speciale evenementen, onderzoeken, wedstrijden en verlotingen.
- We kunnen uw informatie gebruiken om marktonderzoek uit te voeren en deel te nemen aan gezamenlijke promotieactiviteiten met bedrijven die producten hebben die meerwaarde kunnen hebben voor producten of diensten van Lookout (bijvoorbeeld met mobiele operators).

b. We kunnen uw informatie conform de wet vrijgeven

Net als andere bedrijven kunnen we uw informatie vrijgeven conform de wet om, bijvoorbeeld: (i) een wet, regel of wettelijk proces na te leven (inclusief om te voldoen aan nationale veiligheids- of rechtshandhavingsvereisten); (ii) de veiligheid van een persoon, entiteit of faciliteit te beschermen; (iii) potentiële overtredingen van ons privacybeleid of Servicevoorwaarden aan te pakken; (iv) fraude, beveiligingsproblemen of technische problemen te onderzoeken; of (v) de rechten of eigendommen van Lookout of een derde partij, onze werknemers, gebruikers en het publiek te beschermen.

Wij zijn van mening dat u het recht hebt te weten of we wettelijk verplicht zijn uw informatie vrij te geven. Daarom stellen wij u, voordat we uw informatie vrijgeven in reactie op een verzoek van een wetshandhavingsinstelling (bijvoorbeeld een dagvaarding of gerechtelijk bevel), via het e-mailadres dat is vermeld in uw account op de hoogte, tenzij (a) dit verboden is of (b) in noodgevallen waar melden een risico op verwonding of overlijden kan vormen, of als de zaak mogelijke schade voor minderjarigen betekent. Daarnaast is niets in dit privacybeleid bedoeld als beperking van juridische verdediging of bezwaren die u hebt met betrekking tot het verzoek van een derde partij, inclusief van de overheid, om uw informatie vrij te geven.

c. We delen uw informatie om onze diensten te leveren of te verbeteren

We delen uw informatie met andere leden van onze zakelijke groep, of met derde partijen om onze diensten te leveren of verbeteren. Bijvoorbeeld:

- We kunnen uw informatie delen met derde serviceleveranciers van producten en diensten die zijn geïntegreerd met onze software die uw informatie moeten kennen om aan uw verzoek om producten of diensten te kunnen voldoen (bijvoorbeeld om uw locatie in kaart te brengen, u een sms te sturen of u te voorzien van identiteitsbeschermingsdiensten), onze producten en diensten te ondersteunen of gegevens te analyseren voor doeleinden van productprestaties en productverbetering.
- We kunnen uw informatie delen met mobiele operators die deelnemen aan ons Mobile Operator Customer Care-programma zodat zij u via onze Customer Care Web-applicatie direct kunnen helpen met de functies van Lookout Missing Device, zoals extern opsporen, vergrendelen, wissen of Scream, op uw verzoek.
- We kunnen uw informatie delen om boekhouding, audits, facturering en verzamelingsactiviteiten uit te voeren.
- We kunnen uw informatie delen met onze filialen, resellers of andere derde serviceleveranciers die met Lookout werken (bijvoorbeeld mobiele operators en MDM-leveranciers) om te zorgen voor de

juiste levering van uw aankoop en gerelateerde ondersteuningsdiensten, het uitvoeren van aan het bedrijf gerelateerde functies, en het verstrekken van informatie aan u over producten en diensten.

13. Uw gegevens kunnen worden opgenomen in beveiligingsrapporten

Voor gegevensanalyse de-identificeren en aggregeren we gegevens en vatten we ze samen. Deze analyses kunnen uw gegevens bevatten. We kunnen uw informatie met uw toestemming vrijgeven. We kunnen uw persoonsgegevens ook delen met derde partijen als we hiervoor uw toestemming hebben.

14. Uw keuzes

a. U kunt uw instellingen inzien en bijwerken

In uw Lookout-account op onze website en/of op de Lookout 'instellingenpagina' op onze mobiele applicatie kunt u bepaalde instellingen bijwerken of aanpassen die van invloed zijn op welke gegevens worden gedeeld met ons (bijvoorbeeld door back-ups van bepaalde soorten gegevens uit te schakelen). Om uw privacy en veiligheid te beschermen, hebben we uw gebruikersnaam en wachtwoord nodig om uw identiteit te verifiëren voordat we u toegang geven tot uw account om wijzigingen aan te brengen. Als u onnauwkeurigheden in uw persoonsgegevens wilt aanpassen of verwijderen, of als u toegang wilt tot de persoonsgegevens die we over u bewaren, neemt u dan contact met ons op via privacy@lookout.com. We reageren binnen 30 dagen op uw toegangsverzoek. In bepaalde situaties kan Lookout echter niet in staat zijn toegang te bieden tot alle persoonsgegevens die we over u bewaren of deze te wissen.

b. Uitschrijven voor e-mails

U kunt zich uitschrijven voor het ontvangen van promotionele communicatie van Lookout via de koppeling uitschrijven die u in iedere e-mail vindt. Hoewel verzoeken tot uitschrijven meestal onmiddellijk worden verwerkt, moet u rekening houden met tien (10) werkdagen voor verwerking van uw verwijdering. Zelfs nadat u zich hebt uitgeschreven voor het ontvangen van promotieberichten van ons, blijft u transactionele en productgerelateerde berichten van ons ontvangen over Lookout-diensten. U kunt zich voor een aantal van deze meldingsberichten uitschrijven in uw accountinstellingen.

c. Persoonlijke reclames

Het kan zijn dat u zich kunt uitschrijven voor het ontvangen van bepaalde persoonlijke reclames van bedrijven die lid zijn van het Network Advertising Inititative of die zich houden aan de zelfregulerende principes voor online gedragsreclames van Digital Advertising Alliance. Ga naar de Uitschrijfpagina voor consumenten van Network Advertising Initiative of de Uitschrijfpagina van Digital Advertising Alliance om u direct uit te schrijven

bij leveranciers die deelnemen aan die programma's. Lookout beheert of regelt deze middelen of de keuzes die adverteerders en anderen via deze middelen bieden niet.

d. Locatie

Als u locatiegegevens verwijdert via uw accountdashboard op Lookout.com, zijn deze niet langer gekoppeld aan uw account en worden ze gede-identificeerd op onze applicatieproductiesystemen.

15. Gegevensbewaarbeleid

Het is ons beleid persoonsgegevens slechts zo lang te bewaren als redelijkerwijs nodig voor het verstrekken van producten en diensten aan u of als anderszins verplicht voor naleving van de wet. We kunnen uw gegevens verwijderen als uw account inactief is en als anderszins vermeld in onze Servicevoorwaarden.

16. Informatie die wordt geplaatst op onze blog en ons community forum is openbaar

Als u een opmerking maakt onder een blog of in andere openbare forums, moet u weten dat alle informatie die u daar verstrekt kan worden gelezen, verzameld of gebruikt door andere gebruikers van die blog, en kan worden gebruikt om u ongevraagde berichten te sturen. Wij zijn niet verantwoordelijk voor de informatie die u verstrekt in deze blogs of voor inhoud die u ontvangt als gevolg van het delen van dergelijke informatie.

17. We nemen beveiliging serieus

Lookout is een beveiligingsbedrijf en het beveiligen van uw gegevens is belangrijk voor ons. Lookout maakt gebruik van commercieel redelijke fysieke, organisatorische en technische beveiligingsmaatregelen om te zorgen voor de juiste technische en organisatorische beveiliging. We gebruiken bijvoorbeeld een combinatie van firewalls, verificatie, fysieke beveiliging en andere beveiligingsmaatregelen om uw account en uw gegevens te beveiligen. Als u gevoelige informatie (bijvoorbeeld creditcardnummer of informatie op basis van locatie) verstrekt op onze website, in de Lookout app of in onze bestelformulieren, dan versleutelen we de overdracht van die gegevens met behulp van Secure Socket Layer-technologie (SSL). We laten externe partijen ook penetratietesten uitvoeren om ons systeem te wapenen tegen een aanval. Lookout onderneemt iedere redelijke inspanning maatregelen te implementeren om te beschermen tegen complexe technologische dreigingen en andere criminele dreigingen, alsmede om te beschermen tegen nalatige werknemers.

Omdat geen enkele verzendmethode via het internet of elektronische opslagmethode 100% veilig is, kunnen we de veiligheid van informatie, gegevens of inhoud die Lookout namens u ontvangt voor uitvoering van de Lookout-diensten of die u aan Lookout verzendt, niet garanderen. Alle dergelijke ontvangst of verzending van

uw informatie wordt gedaan uit uw eigen vrije wil en op uw eigen risico. We kunnen niet garanderen dat dergelijke informatie niet wordt geopend, vrijgegeven, veranderd of vernietigd door een inbreuk op onze fysieke, technische of organisatorische beveiligingsmaatregelen.

Als Lookout wordt geïnformeerd over een beveiligingsinbreuk, proberen we u elektronisch te waarschuwen, zodat u de juiste beschermingsmaatregelen kunt treffen. Lookout plaatst ook een melding op de Lookout-diensten als er een beveiligingsinbreuk optreedt. Afhankelijk van waar u woont, kunt u het recht hebben schriftelijk een melding te ontvangen van een beveiligingsinbreuk.

18. U bent verantwoordelijk voor het onderhouden van de nauwkeurigheid en vertrouwelijkheid van uw e-mailadres en wachtwoord

U hebt de verantwoordelijkheid uw e-mailadres en wachtwoord te allen tijde geheim te houden. We raden u aan een sterk wachtwoord te gebruiken dat u niet voor andere diensten gebruikt. Als u denkt dat uw wachtwoord is uitgelekt, wijzig uw wachtwoord dan onmiddellijk via de website van Lookout of neem contact met ons op via support@lookout.com voor hulp. Het is uw verantwoordelijkheid te zorgen dat het e-mailadres dat is gekoppeld aan uw account up-to-date is. We gebruiken dat e-mailadres om contact met u op te nemen over service-updates, wijzigingen aan onze beleidsregels en accountactiviteiten zoals verzoeken om informatie of opsporingspogingen van uw apparaat. Lookout is niet verantwoordelijk voor persoonsgegevens die worden overgedragen aan een derde partij als gevolg van het verstrekken van een onjuist e-mailadres door een gebruiker.

19. Opmerking voor gebruikers in Californië

a. Niet traceren

Do Not Track is een privacyvoorkeur die gebruikers in hun internetbrowser kunnen instellen. Als een gebruiker het signaal Do Not Track inschakelt, stuurt de browser een bericht naar websites waarin wordt verzocht de gebruiker niet te traceren. Ga voor meer informatie over Do Not Track naar www.allaboutdnt.org. Op dit moment reageren we niet op Do Not Track-browserinstellingen of -signalen. Daarnaast kunnen een aantal van onze derde serviceleveranciers gebruikmaken van standaardtechnologie, zoals cookies, pixel tags en web beacons om informatie te verzamelen over uw internetactiviteiten. Het kan zijn dat u bepaalde cross-site-tracering van derde partijen kunt uitschakelen als beschreven in de paragraaf 'Uw keuzes' hierboven.

20. Internationale bezoekers, het Privacy Shield en AVG

Lookout is een bedrijf dat is gevestigd in San Francisco met servers geplaatst in de Verenigde Staten.

Persoonsgegevens die van gebruikers buiten de Verenigde Staten worden verzameld, worden overgedragen naar de Verenigde Staten. Als u de diensten van Lookout gebruikt van buiten de Verenigde Staten, kan uw informatie worden overgedragen aan en worden opgeslagen en verwerkt in de Verenigde Staten waar onze servers zich bevinden en onze databases worden uitgevoerd. Lookout heeft een certificering conform het Privacy Shield -raamwerk als opgesteld door het Amerikaanse Ministerie van Handel betreffende het verzamelen, gebruiken en bewaren van persoonsgegevens uit de EU-lidstaten en Zwitserland. De Privacy Shield-principes bevatten een reeks vereisten die van toepassing zijn op het gebruik en de behandeling van persoonsgegevens door deelnemende organisaties ontvangen uit de EU en Zwitserland. Door deel te nemen aan het Privacy Shield doen deelnemers de belofte deze principes na te leven die uitvoerbaar zijn onder Amerikaanse wetgeving. Lookout heeft gecertificeerd dat het zich houdt aan de Privacy Shield-principes betreffende melding, keuze, verdere doorgifte, beveiliging, gegevensintegriteit, toegang en uitvoering van dergelijke persoonsgegevens. Ga voor meer informatie over het Privacy Shield en een lijst van entiteiten die op dit moment een certificering hebben onder het Privacy Shield, of om de certificering van Lookout in te zien, naar http://www.privacyshield.gov.

Als vereist in de principes heeft Lookout wanneer het informatie ontvangt onder het Privacy Shield en deze vervolgens overdraagt aan een derde serviceleverancier die optreedt als agent namens Lookout, een bepaalde aansprakelijkheid onder het Privacy Shield indien (i) de agent de informatie verwerkt op een wijze die inconsistent is met het Privacy Shield en (ii) Lookout verantwoordelijk is voor de gebeurtenis die aanleiding geeft tot de schade.

Als u vragen of klachten hebt over de privacypraktijken van Lookout, inclusief vragen betreffende het Privacy Shield, kunt u contact met ons opnemen via privacy@lookout.com of via het postadres onder 'Contact met ons opnemen als u vragen of twijfels hebt.' Wij proberen uw probleem op te lossen.

Als u een inwoner bent van de Europese Unie en niet tevreden bent over de manier waarop we uw klacht over onze privacypraktijken hebben afgehandeld, kunt u verdere hulp inroepen, zonder bijkomende kosten voor u, via ons speciale hulpmechanisme voor het Privacy Shield. U vindt hierover meer informatie op https://www.jamsadr.com/eu-us-privacy-shield. U hebt ook het recht een klacht in te dienen bij de relevante toezichthouder. We moedigen u echter aan eerst contact op te nemen met ons. Wij doen dan ons uiterste best uw probleem op te lossen.

Inwoners van de Europese Unie kunnen ook kiezen voor bemiddeling bij een onopgeloste klacht, maar voor het starten van een dergelijke arbitrageprocedure moet u: (1) contact opnemen met Lookout en ons de kans bieden het probleem op te lossen; (2) hulp vragen bij het speciale onafhankelijke hulpmechanisme van Lookout als hierboven vermeld; en (3) contact opnemen met het Amerikaanse Ministerie van Handel (rechtstreeks of via een Europese toezichthouder op gegevensbescherming) en het Amerikaanse Ministerie

van Handel tijd geven te proberen het probleem op te lossen. Iedere partij is verantwoordelijk voor zijn eigen advocaatkosten. Let erop dat, conform het Privacy Shield, de arbiter(s) alleen individueel-specifieke, niet-geldelijke, redelijke schadeloosstelling kan opleggen om een overtreding van de Privacy Shield-principes op te lossen met betrekking tot het individu. Lookout is onderhevig aan de onderzoeks- en handhavingsbevoegdheden van de Amerikaanse Federal Trade Commission.

Naast de rechten die zijn toegekend onder bovenstaande paragraaf getiteld 'U kunt uw privacy-instellingen inzien en bijwerken', hebben sommige internationale gebruikers (inclusief de gebruikers wier informatie we verzamelen onder het Privacy Shield) bepaalde wettelijke rechten tot toegang tot bepaalde informatie die we over ze bewaren en de verwijdering daarvan aan te vragen. Om deze rechten uit te oefenen, kunnen deze gebruikers met hun verzoek contact met ons opnemen via privacy@lookout.com.

De Europese Unie heeft een stap genomen in de bescherming van het fundamentele recht op privacy van EU-inwoners met de Algemene Verordening Gegevensbescherming (AVG) die van kracht is vanaf 25 mei 2018. Iedere organisatie die op enigerlei wijze werkt met de persoonsgegevens van een inwoner van de EU, heeft verplichtingen die gegevens te beschermen. Lookout onderneemt iedere commercieel redelijke stap, inclusief aanbevolen technische en organisatorische maatregelen om te voldoen aan de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) (“AVG”).

Onder deze inspanningen vallen:

Identificeren van persoonsgegevens: Voor iedere Lookout-dienst is een ander niveau aan verzameling, gebruik, opslag en verwijderen van persoonsgegevens nodig. Het bepalen van de omvang van de persoonsgegevens voor ieder van deze diensten en het documenteren van de verschillende gegevensbronnen bieden inzicht in welke persoonsgegevens we verzamelen en bieden Lookout de mogelijkheid deze kritieke bedrijfsbron passend te beheren en beschermen.

Bieden van inzicht en transparantie: Lookout biedt transparantie en toegang tot persoonsgegevens door tijdig te reageren op verzoeken van klanten in overeenstemming met de vereisten in de AVG. Verzoeken kunnen worden ingediend door contact op te nemen met support@lookout.com. Persoonsgegevens kunnen worden ingezien en bijgewerkt via uw persoonlijke Lookout-internetportaal.

Zorgen voor integriteit en veiligheid van gegevens: Om gegevensintegriteit te behouden, beheert Lookout toegang tot klantgegevens via strikte toegangscontroles. Lookout implementeert ook passende veiligheidsmaatregelen door persoonsgegevens die worden verzonden en bewaard te versleutelen.

21. Gebruikers jonger dan 16 jaar

Omdat Lookout diensten biedt aan een internationale klantengroep verzamelt of bewaart Lookout, om te

voldoen aan zowel Amerikaanse als Europese vereisten in zowel Hoofdstuk 91 van de Wet Online privacy van kinderen en artikel 8 Voorwaarden van toepassing op toestemming van kinderen met betrekking tot informatiemaatschappijdiensten van de AVG, niet bewust persoonsgegevens over kinderen jonger dan 16 jaar, tenzij zij onderdeel zijn van een Plan voor meerdere apparaten dat is aangeschaft door een ouder die toestemming geeft voor dergelijke verzameling en opslag als beschreven in de Servicevoorwaarden van Lookout. Als u denkt dat een kind deze dienst gebruikt zonder ouderlijke toestemming, neemt u dan contact met ons op via privacy@lookout.com.

22. Wij zijn niet verantwoordelijk voor inhoud op websites van derden

Onze site bevat koppelingen naar andere websites. Als u op een van deze koppelingen klikt, verlaat u de website van Lookout en gaat u ergens anders heen. Lookout aanvaardt geen aansprakelijkheid voor misbruik van informatie door een websitebeheerder waar we naar koppelen. We raden u aan de privacyverklaringen van deze gekoppelde sites te lezen, die kunnen verschillen van die van ons. Daarnaast, als u gebruik maakt van een aanbieding van een van onze partners, kunt u informatie direct aan die partner verstrekken. We raden u aan de privacyverklaringen van deze partners te lezen, omdat wij niet verantwoordelijk zijn voor de privacypraktijken van partners of gekoppelde sites.

23. Wijziging van zeggenschap

In het geval dat Lookout betrokken is bij een faillissement, fusie, acquisitie, reorganisatie of verkoop van activa, kan uw informatie worden verkocht of overgedragen als onderdeel van die transactie.

24. We plaatsen updates op onze websites wanneer dit beleid verandert

Dit privacybeleid kan worden aangepast aan de wijzigingen in onze producten en diensten en wetten die van toepassing zijn op Lookout en u. Als we substantiële wijzigingen aanbrengen aan dit beleid, dan stellen we u hiervan op de hoogte in onze applicatie, hier op de website, via e-mail of door middel van een melding op de startpagina van Lookout. Let erop dat door blijvend gebruik van onze diensten u aangeeft dat u akkoord gaat met, en instemt te zijn gebonden aan, het nieuwe privacybeleid. Als u niet akkoord gaat met het herziene privacybeleid, moet u uw account sluiten.

25. Contact met ons opnemen bij vragen of twijfels

Neemt u contact op met onze privacyfunctionaris op privacy@lookout.com, of via post naar Lookout, Inc., T.a.v.: Michael Musi, Data Privacy Officer, One Front Street, Suite 3100, San Francisco, CA 94111, Verenigde Staten, met vragen of opmerkingen over dit beleid. Inwoners van de EU kunnen ook contact opnemen door vragen te sturen ter attentie van Dhr. G.J. Schenk, SVP, Florapark 3, 2012 HK, Haarlem.