Lookout, Inc.
Personal App
Privacyverklaring

Ingangsdatum: 1/1/2020
Creatiedatum: 15/11/2016
Revisiedatum: 1/1/2023

1. Inleiding

Dit document is onze Privacyverklaring Personal App (de "Verklaring") waarin wordt beschreven welke informatie we van u verzamelen wanneer u de Lookout Personal App (de "Personal App") gebruikt en hoe we deze informatie gebruiken. Het is belangrijk dat u, behalve de Verklaring, ook de Servicevoorwaarden van Lookout (beschikbaar op www.lookout.com/legal/terms) leest, omdat beide documenten van toepassing zijn op uw gebruik van de Personal App. Op informatie over u die Lookout op een andere manier verzamelt dan via het gebruik van de Personal App is een andere privacyverklaring van toepassing.

Deze Verklaring kan worden aangepast aan de wijzigingen in onze producten en diensten en wetten die van toepassing zijn op Lookout en u. Bij wezenlijke veranderingen in deze Verklaring zullen we u op de hoogte stellen. Als u niet akkoord gaat met de herziene Verklaring, moet u uw account sluiten.

U kunt deze Verklaring inzien op het aanmeldscherm van de mobiele applicatie van Lookout, vanuit de instellingen in de Lookout Personal App en op de website van het bedrijf.

2. Informatie die wij verzamelen.

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

a. Informatiecategorieën. Lookout of de partners van Lookout kunnen de volgende categorieën informatie van u verzamelen tijdens uw gebruik van de Personal App:

i. ***Registratiegegevens,*** waaronder een e-mailadres en een wachtwoord.

ii. ***Apparaatgegevens,*** zoals een apparaatidentificator (bijv. mobiel telefoonnummer, apparaattype en -producent, type en versie besturingssysteem, draadloze provider/operator, netwerktype, land van herkomst, SSID van wifinetwerk, Internet Protocol- (IP)-adres en de datums en tijden van uw verzoeken.

iii. ***Applicatiegegevens,*** waaronder metadata van alle applicaties die zijn geïnstalleerd op uw mobiele apparaat (inclusief maar niet beperkt tot de namen van de apps en de versies van de apps), en in bepaalde gevallen kunnen we ook een kopie van gedeeltes van of volledige applicatiebestanden op uw apparaat verzamelen als we een app ontdekken die we niet eerder hebben geanalyseerd. Deze gegevens worden gepseudonimiseerd en in samengevoegde indeling bewaard om te zorgen dat een individu niet kan worden onderscheiden van andere klanten. We kunnen ook informatie verzamelen over hoe applicaties zich gedragen op uw apparaat (bijv. of een applicatie tekstberichten verzendt tegen verhoogd tarief, waardoor uw telefoonrekening kan stijgen) en de netwerkdiensten waarmee uw applicaties communiceren.

iv. ***Locatiegegevens.*** Sommige functies die we aanbieden, werken beter als we beschikken over de locatie van uw mobiele apparaat. 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 we kunnen, in sommige gevallen, locatiegegevens afleiden van een mobiele zendmast of wifihotspot-informatie. We kunnen een beroep doen op derde dienstverleners 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. Dit kan echter wel invloed hebben op de functies die Lookout aanbiedt.

v. ***Gegevens van Diefstalmeldingen,*** waaronder Locatiegegevens en een afbeelding die wordt gemaakt wanneer de functie Theft Alerts wordt ingeschakeld.

vi. ***Betalingsgegevens,*** waaronder uw creditcardnummer, vervaldatum, veiligheidscode en andere toepasselijke factureringsgegevens, kunnen rechtstreeks worden verzameld door de partners van Lookout als u de Premium- en Premium Plus-versies van de app hebt gekocht.

vii. ***Webcontentgegevens***, waaronder URL's en domeinen voor schadelijke content en content die aanvullende analyse vereist om vast te stellen of die URL's onveilig zijn (bijv. of de URL's phishingaanvallen of malware bevatten). Lookout verzamelt uw surfgeschiedenis niet.

viii. ***Gegevens voor Bescherming tegen Identiteitsdiefstal,*** die u kunt verstrekken als u Lookout Premium Plus hebt gekocht, waaronder privé-informatie (zoals rijbewijsnummer, burgerservicenummer, paspoortnummer of andere identificatienummers), financiële informatie (zoals bankrekening, nummers van betaalpas en creditcard); medisch verzekeringsnummer en andere gegevens over u, zoals naam en titel (of andere mensen die u inschrijft voor de dienst), kunnen rechtstreeks worden verzameld door de partner van Lookout, CSIdentity (tegenwoordig onderdeel van Experian).

ix. ***Analytische Gegevens****,* waaronder tools van derden zoals Mixpanel, Braze en mParticle om ons te helpen bij het analyseren en samenvoegen van gegevens over uw gebruik van onze Services. We raden u aan het Privacybeleid van MixPanel, het Privacybeleid van Braze en het Privacybeleid van mParticle te lezen.

Aangezien de productfuncties per laag verschillen, kan Lookout verschillende soorten informatie verzamelen, afhankelijk van de laag die u gebruikt (hieronder verder uitgelegd).

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

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

ii. ***Apparaatgegevens.*** Wanneer u Services van Lookout gebruikt, leggen onze servers bepaalde informatie vast over uw mobiele apparaat, zoals uitgelegd in artikel 2(a)(ii) hierboven.

iii. ***Applicatiegegevens.*** Wanneer u Services van Lookout gebruikt, verzamelen we applicatiebestanden en downloaden we een kopie van gedeeltes van of volledige applicatiebestanden op uw apparaat als we een applicatie ontdekken die we niet eerder hebben geanalyseerd, zoals beschreven in artikel 2(a)(iii) hierboven. Voor de duidelijkheid, Lookout verzamelt geen gebruikersgegevens die u invoert in die applicaties. Lookout verzamelt geen gebruikersgegevens die u invoert in de applicaties op uw mobiele apparaat. Dit betekent dat Lookout geen e-mails of tekstberichten van u verzamelt, leest, controleert of scant. Lookout verzamelt geen foto's of video's van u, maar kan deze bestanden lokaal op het apparaat scannen om u te beschermen tegen bepaalde dreigingen die verborgen zijn in foto- of videobestanden.

iv. ***Locatiegegevens.*** Als de functie Missing Device van Lookout is ingeschakeld, inclusief de Locate and Scream-optie om uw telefoon op afstand te vinden, gebruikt deze Locatiegegevens om u te helpen uw telefoon dichtbij de laatst bekende locatie te vinden als u hem verliest en de batterij leeg is. Als u daarnaast Signal Flare hebt ingeschakeld, verzamelt deze functie Locatiegegevens en stuurt deze terug naar Lookout als de batterij bijna leeg is.

c. Informatie die Lookout verzamelt voor de Lookout Premium Personal App

Lookout verzamelt dezelfde informatie als voor de Lookout Basic Personal App, maar daarnaast verzamelt de partner van Lookout ook rechtstreeks Betalingsgegevens van u om u toegang te bieden tot premiumfuncties, Webcontentgegevens om de functie Safe Browsing te gebruiken en Gegevens over Diefstalmeldingen om de Theft Alerts-functie aan te bieden, zoals hieronder beschreven.

i. ***Betalingsgegevens.*** Als u rechtstreeks bij ons een abonnement afneemt voor Premium of Premium Plus Lookout Services gebruiken we een derde betalingsverwerker voor het verzamelen van uw Betalingsgegevens. Deze verwerker gebruikt die informatie om de diensten bij u in rekening te brengen. 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. Om onze diensten aan u te verlenen, stuurt de App Store Lookout een bevestiging van uw aankoop. Providers kunnen uw telefoonnummer, abonnement-ID, SKU en andere niet-financiële informatie delen. De App Store en uw provider delen geen creditcard- of factuurinformatie. Raadpleeg voor aanvullende informatie het beleid en de procedures voor betalingsverwerking van uw App Store of provider.

ii. ***Webcontentgegevens.*** Lookout gebruikt Webcontentgegevens om de Safe Browsing-dienst aan te bieden. Als u niet wilt dat wij de door u bezochte onveilige URL's documenteren, kunt u Safe Browsing uitschakelen; alle andere functies van Lookout blijven dan gewoon functioneren.

iii. ***Gegevens over Diefstalmeldingen.*** Als Theft Alerts wordt geactiveerd, 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. Vervolgens wordt de foto 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.

d. Informatie die Lookout verzamelt voor de Lookout Premium Plus Personal App

Lookout verzamelt dezelfde informatie als voor de Lookout Premium Personal App, maar daarnaast verzamelt de partner van Lookout ook Gegevens voor Bescherming tegen Identiteitsdiefstal van u.

i. ***Gegevens voor Bescherming tegen Identiteitsdiefstal.*** Wanneer u de Identity Theft Protection-functie gebruikt, kunt u de bovengenoemde Gegevens voor Bescherming tegen Identiteitsdiefstal gebruiken om u aan te melden voor bepaalde identiteitsbeschermingsdiensten die onze partner CSIdentity (tegenwoordig onderdeel van Experian) aanbiedt. Welke informatie CSIdentity over u verzamelt en bewaart, is afhankelijk van de informatie die u hebt ingevoerd in de Personal App. CSIdentity kan genoodzaakt zijn uw Gegevens voor Bescherming tegen Identiteitsdiefstal te verstrekken aan derde dienstverleners (zoals identificatieverificatiebedrijven, consumentenrapportagebureaus, kredietcontrolebureaus, betalingscontrolebedrijven, wetshandhavingsinstellingen en anderen) om u die diensten te kunnen leveren.

e. Informatie die Lookout verzamelt uit bronnen van derden

Lookout ontvangt Analytische Gegevens van derden, zoals hierboven uitgelegd.

3. Hoe we uw informatie gebruiken.

Als we uw informatie verzamelen, slaan we deze op en koppelen we deze aan uw account, tenzij anders vermeld. Merk op dat we bepaalde soorten informatie nodig hebben om de diensten aan u te kunnen verlenen. 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 diensten. We nemen uw privacy zeer serieus en we gebruiken en geven uw informatie alleen vrij voor de zakelijke en commerciële doeleinden die in deze Verklaring worden beschreven. Hoe we uw informatie gebruiken, is afhankelijk van het type gegevens zoals hieronder uitgelegd:

a. Applicatiegegevens. We gebruiken deze gegevens om onze diensten te verlenen door scans van applicatiebestanden uit te voeren, met als doel vast te stellen of applicaties schadelijk gedrag vertonen. Ook pseudonimiseren we gegevens en voegen deze samen om de populariteit van toepassingen per regio vast te stellen en onze mobiele dreigingsanalyse uit te voeren. De gegevens van de mobiele dreigingsanalyse blijven gepseudonimiseerd om de privacy van gegevens te waarborgen. Door klantgegevens op een veilige en vertrouwelijke manier te combineren, krijgt Lookout meer inzicht in de huidige beveiligingsdreigingen en kunnen de Lookout-diensten worden verbeterd.

b. Apparaatgegevens. Er kunnen periodiek automatische scans van uw apparaat worden uitgevoerd 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 Personal App toe te staan om dreigingen op uw mobiele apparaat te detecteren en aanpakken. Voor zover beschikbaar kan Lookout informatie van clientapparaten gebruiken om u te laten weten dat u uw besturingssysteem moet bijwerken. Behalve de informatie die u aan ons verstrekt en de informatie die we verzamelen van uw mobiele eindpuntapparaat om de Lookout-diensten te kunnen 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 optreden 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.

c. **Gegevens voor Bescherming tegen Identiteitsdiefstal.** CSIdentity gebruikt deze informatie om uw identiteit te controleren en de gevraagde identiteitsbeschermingsdiensten aan u te leveren. Als u opwaardeert naar een Premium Plus-abonnement met daarin identiteitsdiefstalverzekering, gebruiken onze partners uw informatie om u te voorzien van hulp en toepasselijke verzekeringsdekking als uw identiteit in gevaar wordt gebracht.

d. **Locatiegegevens.** De functie Missing Device van Lookout bevat de Locate and Scream-optie om uw telefoon op afstand te vinden via uw persoonlijke account op Lookout.com, en Lookout gebruikt Locatiegegevens om u te helpen uw telefoon dichtbij de laatst bekende locatie te vinden als u hem verliest en de batterij leeg is. Als u Signal Flare hebt ingeschakeld, verzamelt deze locatiegegevens en stuurt die gegevens 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 Personal App.

e. **Registratiegegevens.** We kunnen uw e-mailadres of mobiele telefoonnummer gebruiken om u informatie te sturen over productaankondigingen en speciale aanbiedingen van Lookout of onze zakenpartners. Als u Lookout mailt voor hulp, kunnen we die informatie bewaren om u te helpen en om onze diensten te verbeteren. We kunnen uw e-mailadres gebruiken om met uw apparaat te communiceren over de diensten, waaronder door het verzenden van aan privacy of beveiliging gerelateerde meldingen en door u te informeren over grote serviceveranderingen van Lookout.

f. **Gegevens over Diefstalmeldingen**. We gebruiken deze informatie om de diefstalmeldingsdiensten te verlenen.

g. **Webcontentgegevens.** 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. Bezochte URL's worden gepseudonimiseerd en verzonden naar Lookout om beveiligingsscans uit te voeren. We gebruiken het dossier van de onveilige URL's die u bezoekt om u een melding te sturen dat de URL die u probeert te bereiken onveilig is.

4. Hoe we uw informatie vrijgeven

Dit artikel beschrijft hoe Lookout uw informatie kan delen en vrijgeven.

a. **Derde dienstverleners en partners**. We kunnen uw informatie delen met derde dienstverleners van wie de producten en diensten zijn geïntegreerd met onze software en die uw informatie moeten kennen om te voldoen om aan uw verzoek om producten of diensten, onze producten en diensten te ondersteunen of gegevens te analyseren met het oog op productprestaties en productverbetering. Bijvoorbeeld:

   i. Wanneer u de Identity Theft Protection-functie gebruikt, wordt uw informatie verzameld door onze partner CSIdentity (tegenwoordig onderdeel van Experian) om de dienst aan u te verlenen. CSIdentity op haar beurt kan uw gegevens verstrekken aan derden, zoals identificatieverificatie-bedrijven, consumentenrapportagebureaus, kredietbureaus, betalingscontrolebedrijven, wetshandhavingsinstellingen en anderen om de gevraagde diensten aan u te verlenen. CSIdentity kan u ook voorzien van bewaking en meldingen, en informatie en rapporten over u opvragen (of over anderen die u hebt ingeschreven) om de identiteitsbeschermingsdiensten aan te bieden, inclusief adresgeschiedenis, naam, alias en andere rapporten. We verplichten CSIdentity en haar dienstverleners de over u verzamelde gegevens alleen te gebruiken voor het verlenen van diensten via het Lookout App Premium Plus Product.

   ii. We kunnen uw informatie delen met onze resellers of andere mobiele operators om te zorgen voor een correcte levering van uw aankoop en gerelateerde ondersteuningsdiensten en voor het uitvoeren van bedrijfsgerelateerde functies.

   iii. We kunnen uw informatie gebruiken om marktonderzoek uit te voeren en deel te nemen aan gezamenlijke promotieactiviteiten met bedrijven waarvan de producten meerwaarde kunnen hebben voor producten of diensten van Lookout (bijvoorbeeld met mobiele operators).

b. **Derde betalingspartners**. We kunnen dienstverleners toestaan rechtstreeks informatie van u te verzamelen om boekhoudings-, controle-, facturerings- en verzamelingswerkzaamheden uit te voeren.

c. **Om de wet na te leven**. We kunnen uw informatie vrijgeven wanneer dat wettelijk is toegestaan, bijvoorbeeld om: (i) een wet, voorschrift of wettelijke procedure na te leven (waaronder om te voldoen aan nationale veiligheids- of wetshandhavingsvereisten); (ii) de veiligheid van een persoon, entiteit of faciliteit te beschermen; (iii) potentiële overtredingen van onze Verklaring 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 waarin deze mededeling een risico op verwonding of overlijden kan veroorzaken, of als de zaak mogelijke schade voor minderjarigen behelst. Verder beperkt niets in deze Verklaring uw wettelijke recht op verdediging of bezwaren die u kunt hebben ten aanzien van het verzoek van een derde partij, waaronder de overheid, om uw informatie vrij te geven.

d. **Tijdens een verandering in de activiteiten van Lookout**. We kunnen uw informatie ook vrijgeven aan een (potentiële) koper en aan zijn vertegenwoordigers of adviseurs in het kader van een (voorgestelde) aankoop, fusie of overname van enig onderdeel van ons bedrijf, mits we de koper meedelen dat hij uw informatie uitsluitend mag gebruiken voor de in deze Verklaring beschreven doeleinden.

e. **Gepseudonimiseerde en samengevoegde gegevens**. Voor gegevensanalyse kunnen we gegevens, waaronder die van u, pseudonimiseren, samenvoegen en samenvatten. Rapporten die voortvloeien uit de analyse van deze gegevens kunnen we publiceren om anderen te helpen inzicht te krijgen in mobiele dreigingen en in specifiek gedrag van mobiele apps.

f. **Met toestemming**. We kunnen uw informatie ook vrijgeven aan derde partijen als u ons hiervoor toestemming hebt gegeven.

5. Uw keuzes

a. U kunt uw instellingen inzien en bijwerken

U kunt de instellingen van uw Lookout-account bijwerken via de instellingenpagina in onze mobiele app of door in te loggen op onze website https://my.lookout.com/user/login. Zo kunt u instellingen wijzigen die bepalen welke gegevens met ons worden gedeeld. Om uw privacy en veiligheid te beschermen, hebben we uw gebruikersnaam en wachtwoord nodig om uw identiteit te verifiëren voordat we u toegang geven of voordat u wijzigingen kunt aanbrengen in uw account.

b. Uitschrijven voor e-mails

U kunt zich uitschrijven voor het ontvangen van promotionele communicatie van Lookout via de koppeling voor 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 promotieberichten van ons, blijft u transactionele en productgerelateerde berichten van ons ontvangen over Lookout Services. U kunt zich voor een aantal van deze meldingen uitschrijven in uw accountinstellingen.

6. Bewaren van gegevens

Lookout bewaart uw informatie, waaronder uw Persoonsgegevens (volgens de definitie van deze term in de AVG) slechts zo lang als redelijkerwijs nodig is voor het aanbieden van producten en diensten aan u of als anderszins vereist om de wet na te leven.

7. Beveiliging

a. Verantwoordelijkheden van Lookout.

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, afgestemd op het risico van de verwerking van uw informatie. 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 (zoals Locatiegegevens) invoert in de Lookout-app, versleutelen we die informatie tijdens overdracht en in rust met behulp van Secure Socket Layer-technologie (SSL). We laten externe partijen ook penetratietesten uitvoeren om ons systeem te wapenen tegen een aanval. Lookout verricht alle redelijke inspanningen voor het implementeren van controlemaatregelen ter bescherming tegen complexe technologische dreigingen en andere criminele dreigingen, alsmede om te beschermen tegen nalatige werknemers.

Daar 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 verstrekt, niet garanderen. Elke 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 die gevolgen voor u kan hebben, proberen we u elektronisch te waarschuwen, zodat u de juiste beschermingsmaatregelen kunt treffen. Lookout plaatst ook een melding op de Lookout Services als er een beveiligingsinbreuk optreedt. Afhankelijk van waar u woont, kunt u het recht hebben schriftelijk een melding te ontvangen van een beveiligingsinbreuk.

b. Uw verantwoordelijkheden.

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 pogingen om uw apparaat op te sporen. Lookout is niet verantwoordelijk voor informatie die wordt overgedragen aan een derde partij als gevolg van het verstrekken van een onjuist e-mailadres door een gebruiker.

8. Gebruikers jonger dan 16 jaar

Lookout verzamelt of bewaart niet bewust persoonsgegevens van 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 zoals 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.

9. Internationale gegevensoverdrachten

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 Services van Lookout buiten de Verenigde Staten gebruikt, kan uw informatie worden overgedragen aan en worden opgeslagen en verwerkt in de Verenigde Staten, waar onze servers zich bevinden en onze databases worden beheerd.

10. Aanvullende voorwaarden voor inwoners van Californië

a. Persoonsgegevens.

In overeenstemming met de California Consumer Privacy Act (“CCPA”), zoals gewijzigd door de California Privacy Rights Act, vindt u hieronder een lijst met de categorieën persoonsgegevens (volgens de definitie van deze term in de CCPA) die we verzamelen (hetzij via de Personal App of elders), de categorieën bronnen waaruit we ze verzamelen, de commerciële doeleinden waarvoor de gegevens zijn verzameld en de categorieën van derden waarmee we de persoonsgegevens delen. De informatie in de onderstaande tabel is correct voor de voorgaande twaalf maanden.

Categorieën persoonsgegevens	Categorieën bronnen	Commerciële doeleinden	Categorieën van entiteiten aan wie we Persoonsgegevens verkopen, delen of bekendmaken voor zakelijke doeleinden
Identificatiegegevens, waaronder e-mailadres, IP-adres, SSID van wifinetwerk en andere apparaat-id's	Consument	Diensten verlenen, diensten verbeteren, klantenservice, analyse	Gegevensanalyseproviders, serviceproviders en contractanten
*Identificatiegegevens voor bescherming tegen identiteitsdiefstal, waaronder SSN, rijbewijsnummer, creditcard- en bankrekeningnummers	Consument	Diensten verlenen	Serviceproviders en contractanten
Geolocatiegegevens	Consument	Diensten verlenen	Serviceproviders en contractanten
Informatie over de interactie van een consument met websites of toepassingen	Consument	Diensten verlenen	Serviceproviders en contractanten

*Alle identificatiegegevens voor bescherming tegen identiteitsdiefstal worden rechtstreeks door de consument ingevoerd, worden opgeslagen door de externe serviceprovider van Lookout, CSID (nu onderdeel van Experian) en worden uitsluitend gebruikt voor het verlenen van de diensten.

b. Uw rechten.

In overeenstemming met de CCPA, en onder voorbehoud van uitzonderingen, hebben consumenten in Californië (volgens de definitie van deze term in de CCPA) de volgende rechten:

i. **Toegang.** U hebt het recht te verzoeken dat Lookout de categorieën Persoonsgegevens die Lookout over u heeft verzameld, of de specifieke stukken Persoonsgegevens die het bedrijf over u heeft verzameld, openbaar maakt en verstrekt;

ii. **Verwijdering.** U hebt het recht te verzoeken dat Persoonsgegevens over u in bepaalde situaties worden verwijderd, met inachtneming van bepaalde uitzonderingen die in de wet zijn vastgelegd;

iii. **Correctie.** U hebt het recht de Persoonsgegevens over u in onze bestanden te laten corrigeren of wijzigen;

iv. **Non-discriminatie.** U hebt het recht om niet gediscrimineerd te worden, met inbegrip van maar niet beperkt tot het recht om geen andere prijs bij u in rekening te worden gebracht voor de diensten of geweigerd te worden voor toegang tot de diensten, op basis van uw beslissing om een van uw rechten in dit artikel uit te oefenen. Wij zullen u niet discrimineren vanwege het uitoefenen van een van uw rechten onder de CCPA.

v. **Uitschrijven.** Lookout verkoopt of deelt geen Persoonsgegevens van zijn gebruikers van de Personal App, dus dit recht is niet op u van toepassing.

vi. **Beperking van het gebruik van gevoelige persoonsgegevens.** Lookout verwerkt uw "Gevoelige persoonsgegevens" (volgens de definitie van deze term in de CCPA) niet voor doeleinden die verdergaan dan toegestaan in Sectie 7027(m) van de CCPA-voorschriften, dus dit recht is niet op u van toepassing.

U kunt uw recht uitoefenen om toegang te krijgen tot uw informatie of om uw informatie te verwijderen op twee manieren (1) door het webformulier in te vullen dat toegankelijk is via https://personal.support.lookout.com, of (2) een verzoek sturen naar Privacy@Lookout.com. Zoals hierboven vermeld in artikel 5(a), vereisen we ter bescherming van uw privacy en veiligheid dat u uw identiteit verifieert door u aan te melden bij uw account met uw gebruikersnaam en wachtwoord voordat we uw verzoek om toegang tot of verwijdering van uw Persoonsgegevens inwilligen. Als we uw identiteit niet kunnen verifiëren, geven we geen specifieke stukken Persoonsgegevens vrij als reactie op een toegangsverzoek, en weigeren we uw verzoek om Persoonsgegevens te verwijderen als reactie op

een verwijderingsverzoek. Voor verzoeken om uw informatie te verwijderen, gebruikt Lookout een tweestapsproces waarbij u eerst duidelijk het verzoek tot verwijdering moet indienen en vervolgens afzonderlijk moet bevestigen dat u uw Persoonsgegevens wilt laten verwijderen. Als consument in Californië kunt u een gemachtigde namens u een toegangs- of verwijderingsverzoek laten doen, op voorwaarde dat de gemachtigde uw schriftelijke toestemming heeft en u uw eigen identiteit rechtstreeks kunt verifiëren met Lookout.

11. Aanvullende voorwaarden voor inwoners van de Europese Economische Ruimte ("EER")

a. Rechtsgrond voor de verwerking.

Als u een bezoeker uit de EER bent, is Lookout de verwerkingsverantwoordelijke van uw Persoonsgegevens (volgens de definitie van deze term in de Algemene Verordening Gegevensbescherming (AVG)). De rechtsgrond voor het verzamelen en gebruiken van uw persoonsgegevens zoals beschreven in deze Verklaring is afhankelijk van de betreffende Persoonsgegevens en de specifieke context waarin we deze verzamelen. Echter, we verzamelen normaal gesproken alleen Persoonsgegevens van u wanneer: (a) het gebruik van uw Persoonsgegevens noodzakelijk is om onze verplichtingen na te komen op grond van een contract met u (bijvoorbeeld voor de naleving van de Servicevoorwaarden die u accepteert door onze apps te downloaden en gebruiken); (b) het gebruik van uw Persoonsgegevens nodig is voor onze gerechtvaardigde belangen of de gerechtvaardigde belangen van anderen (bijvoorbeeld om te zorgen voor de beveiliging van de Lookout Services, het uitvoeren en op de markt brengen van de Lookout Services, het 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 Services leveren); of (c) we hiervoor toestemming van u hebben gekregen (bijvoorbeeld voor sommige van onze marketingactiviteiten). Sommige verwerkingsactiviteiten worden uitgevoerd om te voldoen aan toepasselijke wetgeving.

b. Privacyschild

Lookout heeft een zelfcertificering conform het EU-VS-privacyschild- en Zwitserland-VS-privacyschild-raamwerk, opgesteld door het Amerikaanse Ministerie van Handel betreffende het verzamelen, gebruiken en bewaren van persoonsgegevens uit de EU-lidstaten, het Verenigd Koninkrijk en Zwitserland. Deze raamwerken zijn ontwikkeld om bedrijven in staat te stellen zich aan de gegevensbeschermingseisen te houden wanneer ze persoonsgegevens vanuit de Europese Unie, het Verenigd Koninkrijk en Zwitserland overbrengen naar de Verenigde Staten. Ga voor meer informatie over het Privacyschild en een lijst van entiteiten die op dit moment zijn gecertificeerd conform het Privacyschild naar http://www.privacyshield.gov.

De beginselen bepalen dat, wanneer Lookout informatie ontvangt die onder het Privacyschild valt en deze vervolgens overdraagt aan een derde dienstverlener die optreedt als vertegenwoordiger namens Lookout, Lookout een zekere aansprakelijkheid op grond van het Privacyschild heeft indien (i) de vertegenwoordiger de informatie verwerkt op een wijze die niet conform is met het Privacyschild en (ii) Lookout verantwoordelijk is voor de gebeurtenis die aanleiding geeft tot de schade.

Ten aanzien van persoonsgegevens die worden ontvangen of overgedragen krachtens de Privacyschild-raamwerken zijn we onderhevig aan de onderzoeks- en handhavingsbevoegdheden van de Amerikaanse Federal Trade Commission. In sommige situaties kunnen we verplicht zijn om persoonsgegevens te onthullen als antwoord op rechtmatige verzoeken van overheidsinstanties, waaronder om te voldoen aan nationale veiligheids- of wetshandhavingsvereisten.

Als u niet tevreden bent over de manier waarop we uw klacht over onze privacypraktijken hebben afgehandeld en wij uw persoonsgegevens verwerken in overeenstemming met het Privacyschild, kunt u verdere hulp inroepen, zonder bijkomende kosten voor u, via ons speciale onafhankelijke verhaalmechanisme onder het Privacyschild. 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. U kunt ook kiezen voor bindende arbitrage bij een onopgeloste klacht, maar voorafgaand aan 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 via het speciale onafhankelijke verhaalmechanisme van Lookout, zoals 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 om te proberen het probleem op te lossen. Raadpleeg https://www.privacyshield.gov/article?id=ANNEX-I-introduction voor meer informatie over de bindende arbitrageregeling van het Privacyschild. Iedere partij is verantwoordelijk voor zijn eigen advocaatkosten. Let erop dat, conform het Privacyschild, de arbiter(s) alleen individuspecifieke, niet-geldelijke, redelijke schadeloosstelling kan/kunnen opleggen om een overtreding van de beginselen van het Privacyschild op te lossen met betrekking tot het individu. Lookout is onderhevig aan de onderzoeks- en handhavingsbevoegdheden van de Amerikaanse Federal Trade Commission.

Lookout is ervan op de hoogte dat het Hof van Justitie van de Europese Unie (HvJ-EU) het Privacyschild ongeldig heeft verklaard als een certificering van naleving van de EU-privacywetgeving. Lookout heeft zijn verplichtingen altijd onafhankelijk gehandhaafd via het privacybeleid met partners, klanten en gebruikers van onze website. Lookout verbindt zich ertoe te blijven voldoen aan de toepasselijke vereisten voor de bescherming van persoonsgegevens zoals vereist krachtens toepasselijke wet- en regelgeving en andere overheidsinstanties. Lookout heeft verder toegezegd samen te werken met het panel dat is opgericht door de instanties voor bescherming van persoonsgegevens in de EU (DPA's) en de Zwitserse federale commissaris inzake gegevensbescherming en informatie (FDPIC) met betrekking tot onopgeloste Privacyschildklachten over gegevens die zijn overgedragen vanuit de EU en Zwitserland. Lookout zal de ontwikkelingen met betrekking tot het EU-VS-kader voor gegevensprivacy blijven volgen en ervoor zorgen dat de behandeling van persoonsgegevens in overeenstemming is met de toepasselijke wetgeving.

12. Rechten van betrokkenen

Als u inwoner bent van het Verenigd Koninkrijk, de EER of een ander rechtsgebied met een toepasselijke wetgeving inzake gegevensbescherming (zoals Virginia, Colorado, Connecticut en Utah), hebt u mogelijk bepaalde rechten met betrekking tot uw Persoonsgegevens. Deze rechten kunnen onderhevig zijn aan bepaalde uitzonderingen. Onder deze rechten kunnen vallen:

i. **Toegang.** U kunt het recht hebben om een kopie op te vragen van de Persoonsgegevens die we over u verwerken. Als u meer dan één kopie nodig hebt, kunnen we een redelijke vergoeding in rekening brengen;

ii. **Rectificatie.** U kunt het recht hebben om correctie te eisen van fouten (onvolledigheid of onjuistheid) in de Persoonsgegevens die we over u bezitten;

iii. **Verwijdering.** U kunt het recht hebben om te eisen dat de uzelf betreffende Persoonsgegevens in bepaalde situaties worden verwijderd, bijvoorbeeld wanneer we ze niet meer nodig hebben of als u uw toestemming intrekt (indien van toepassing); In aanvulling op de rechten die zijn verleend in het bovenstaande artikel genaamd “U kunt uw instellingen inzien en bijwerken”, kunt u contact met ons opnemen via privacy@lookout.com om verzoeken in te dienen;

iv. **Overdraagbaarheid.** U hebt het recht de u betreffende Persoonsgegevens die u aan ons hebt verstrekt, te ontvangen in een gestructureerd, veelgebruikt en machineleesbaar formaat en die gegevens in bepaalde situaties over te dragen aan een derde;

v. **Bezwaar.** U kunt het recht hebben om (i) op elk moment bezwaar te maken tegen de verwerking van uw Persoonsgegevens voor direct-marketingdoeleinden en (ii) bezwaar te maken tegen de verwerking van uw Persoonsgegevens wanneer de rechtsgrond van die verwerking ons gerechtvaardigd belang of het gerechtvaardigd belang van een derde is.

vi. **Beperking.** U hebt het recht om te eisen dat we onze verwerking van uw Persoonsgegevens in bepaalde omstandigheden beperken, bijvoorbeeld wanneer u de juistheid van die Persoonsgegevens betwist;

vii. **Intrekking van toestemming.** Als we vertrouwen op uw toestemming voor de verwerking van uw Persoonsgegevens, hebt u het recht die toestemming op elk moment in te trekken.

viii. **Een klacht indienen bij een toezichthoudende autoriteit voor gegevensbescherming.** Afhankelijk van uw rechtsgebied kunt u het recht hebben om een klacht in te dienen bij uw lokale toezichthoudende autoriteit voor gegevensbescherming als u van mening bent dat we de toepasselijke wetgeving inzake gegevensbescherming overtreden.

Neem contact met ons op via privacy@lookout.com als u deze rechten wilt uitoefenen. We reageren op uw verzoek binnen de periode die vereist is onder de toepasselijke wetgeving. Houd er rekening mee dat we mogelijk uw identiteit moeten verifiëren voordat we aan uw verzoek kunnen voldoen. We verifiëren uw identiteit door u een e-mail te sturen naar het e-mailadres dat aan uw account is gekoppeld of door u te vragen om aanvullende informatie te verstrekken die aan uw account is gekoppeld. U kunt ook een gemachtigde aanwijzen om namens u een verzoek in te dienen (hoewel we mogelijk nog steeds uw identiteit moeten verifiëren).

13. Contact met ons opnemen bij vragen of twijfels

Neem contact op met onze Functionaris Gegevensbescherming via het e-mailadres privacy@lookout.com of stuur een schrijven naar Lookout, Inc., T.a.v.: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA (USA) 02108, als u vragen of opmerkingen over deze Verklaring hebt. Inwoners van de EER kunnen ook contact opnemen door vragen te sturen ter attentie van Dhr. Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem.