Ondernemingsprivacyverklaring

Ingangsdatum: 24/10/2016
Creatiedatum: 24/10/2016
Revisiedatum: 25/05/2018
Status: Goedgekeurd

Inhoudsopgave

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 huidige 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	24/10/2016	Huidig concept op openbare website	Marcelo Guerra
2.0	01/04/2018	Herzieningen aan beleid om aansluiting met productaanbod te behouden	Kimberly Snow

Privacyverklaring Mobile Endpoint Security

Lookout is van mening dat uw privacy net zo belangrijk is als uw veiligheid, dus willen we volledig transparant zijn over de gegevens die we verzamelen om uw apparaat en de veiligheid van uw werkgever te beschermen. Lookout, Inc. (“Lookout,” “we,” of “ons” of “onze”) verstrekt u deze Ondernemingsprivacyverklaring waarin informatiepraktijken worden beschreven met betrekking tot onze Mobile Endpoint Security-producten (het “Endpoint Security-product”). Deze Ondernemingsprivacyverklaring is van toepassing op de gegevens die van of over u worden verzameld via uw installatie en activering van ons Endpoint Security-product op uw mobiele apparaat. Door het Endpoint Security-product te downloaden en activeren, geeft u toestemming voor de verzameling, het gebruik, de vrijgave en de opslag van gegevens als beschreven in deze Ondernemingsprivacyverklaring.

Het kan zijn dat u instructies hebt ontvangen voor het downloaden en installeren van het Endpoint Security-product als gevolg van uw werkzaamheden bij een organisatie die (1) vereist dat alle of een deel van zijn werknemers het Endpoint Security-product installeert of (2) vereist dat alle of een deel van zijn werknemers een Mobile Device Management-pakket installeert met daarin het Endpoint Security-product. Let erop dat deze Ondernemingsprivacyverklaring alleen van toepassing is op onze informatiepraktijken met betrekking tot ons Endpoint Security-product. Als u vragen of verzoeken hebt met betrekking tot de praktijken voor verzamelen, gebruiken, vrijgeven en beveiligen van gegevens van uw werkgever (“werkgever”) of een mobile device management-leverancier (“MDM-leverancier”) of over de gegevens die we verzamelen namens uw werkgever, moet u deze vragen of verzoeken tot die partijen richten.

Lookout behoudt zich het recht voor deze Ondernemingsprivacyverklaring op ieder moment aan te passen aan wijzigingen in de wet, onze gegevensverzamelings- en gebruikspraktijken, de kenmerken van het Endpoint Security-product of technologische ontwikkelingen. Controleer deze pagina regelmatig op wijzigingen. Als u het Endpoint Security-product blijft gebruiken na het plaatsen van wijzigingen in deze Ondernemingsprivacyverklaring, is dit een acceptatie van die wijzigingen.

We hebben getracht deze Ondernemingsprivacyverklaring zo in te delen dat uw vragen over ons Endpoint Security-product worden beantwoord. De privacyverklaring bevat antwoorden op de volgende vragen:

1. Wat is het Lookout Mobile Endpoint Security-product?

Lookout Mobile Endpoint Security (MES) is een mobiele beveiligingsoplossing die de risico's verkleint van onbeveiligde gegevens die worden geopend via mobiele apparaten. De Lookout Mobile Endpoint Security-oplossing biedt inzicht in mobiele dreigingen in apps, apparaten en het netwerk. Lookout Mobile Endpoint Security integreert naadloos met en verbetert bestaande mobiele investeringen en minimaliseert het aantal problemen dat wordt gemeld bij de helpdesk. Het Lookout MES-platform maakt gebruik van een wereldwijd sensornetwerk van meer dan 100 miljoen sensoren en biedt voorspellende beveiliging door gebruik te maken van kunstmatige intelligentie om complexe patronen te identificeren die duiden op risicopatronen die anders aan de aandacht van menselijke analisten zouden ontsnappen. Als een dreiging is gedetecteerd, biedt Lookout werknemers en beheerders herstelopties (bijv. app verwijderen, voorwaardelijke toegang instellen). Deze oplossing wordt geleverd via de integratie van de Lookout MES met toonaangevende MDM-leveranciers.

2. Welke gegevens verzamelt Lookout van uw mobiele apparaat?

Om uw mobiele apparaat en uw werkgever te beschermen tegen dreigingen, verzamelt Lookout bepaalde categorieën gegevens van uw apparaat. Onder deze gegevens **kunnen** vallen:

- De producent en het model van uw mobiele apparaat
- Bepaalde technische instellingen op uw mobiele apparaat, inclusief de schermafmeting van uw mobiele apparaat en firmware-versie
- Uw IP-adres (dat uw land en geolocatie kan aanduiden)
- Het soort en de versie van het besturingssysteem op uw mobiele apparaat
- De unieke apparaatidentificatiecode van uw mobiele apparaat
- Configuratiegegevens van uw apparaat, zoals of uw apparaat is geconfigureerd voor root-toegang of dat de hardwarebeperkingen van het apparaat zijn verwijderd
- 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)
- Metadata over netwerken waarmee uw mobiele apparaat verbinding maakt (inclusief maar niet beperkt tot SID van het netwerk of het unieke MAC-/BSSID-adres van uw netwerkapparatuur)

- Onder bepaalde omstandigheden kunnen we ook een kopie van de applicatie verzamelen
- Gegevens van tracking tools die worden gebruikt voor het analyseren van productprestaties op uw apparaat
- Hoe u reageert op meldingen van Lookout dat bepaalde applicaties een beveiligingsrisico kunnen vormen

Als u de functie Privacy Controls in ons Mobile Enterprise Security-product gebruikt in combinatie met een MDM-leverancier, verzamelen we geen persoonsgegevens zoals gebruikersnaam of e-mailadres.

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

3. Als Lookout informatie verzamelt over applicaties die zijn geïnstalleerd op mijn apparaat, betekent dat dat Lookout mijn e-mails leest of mijn foto's bekijkt?

Nee. Lookout verzamelt alleen metadata over applicaties op uw apparaat, of de applicatie zelf. Lookout verzamelt geen gebruikersgegevens die u invoert in die applicaties. Omdat Lookout geen gebruikersgegevens verzamelt die u in de applicaties op uw mobiele apparaat invoert, verzamelt, leest, controleert of scant Lookout uw e-mails, tekstberichten, foto's of video's niet.

4. Verzamelt Lookout andere gegevens over mij buiten mijn mobiele apparaat?

Voor ons Mobile Endpoint Security-product moeten alle mobiele apparaten van werknemers zijn gekoppeld aan een specifiek e-mailadres als het is geïnstalleerd zonder integratie met een MDM-leverancier. Daarom kan uw werkgever Lookout uw e-mailadres verstrekken om MES-diensten te activeren. Als het Lookout Endpoint Security-product is geïntegreerd met een MDM-oplossing en Privacy Controls zijn ingeschakeld, verzamelt Lookout uw e-mailadres niet.

Als u het Mobile Endpoint Security-product hebt geïnstalleerd als onderdeel van een product van een MDM-leverancier, kunnen we ook informatie over u verzamelen bij die MDM-leverancier. Neem contact op met de relevante MDM-leverancier betreffende de privacypraktijken van die leverancier.

Lookout kan ook andere informatie over u verzamelen als u dergelijke informatie rechtstreeks aan ons verstrekt door contact met ons op te nemen en vrijwillig dergelijke informatie vrij te geven, of door uw informatie te verstrekken aan derde partijen zoals onze partners en marketeers. We kunnen deze informatie gebruiken om u te voorzien van updates over Lookout en onze producten en diensten. We kunnen u ook uitnodigen voor conferenties en andere evenementen waaraan Lookout kan deelnemen of die Lookout kan organiseren.

5. Wanneer verzamelt Lookout gegevens van mijn mobiele apparaat?

Zoals hierboven beschreven verzamelt Lookout uw e-mailadres van uw werkgever als het Mobile Endpoint Security-product wordt geïnstalleerd zonder een MDM. Als het Mobile Endpoint Security-product is geïnstalleerd in combinatie met een MDM-oplossing en Privacy Controls zijn ingeschakeld, verzamelt Lookout uw e-mailadres niet. Nadat u het Mobile Endpoint Security-product hebt gedownload, geïnstalleerd en geactiveerd, begint Lookout onmiddellijk met het verzamelen van gegevens van uw apparaat. Als u applicaties op uw mobiele apparaat installeert of opent, scannen we die applicaties op mogelijke beveiligingsdreigingen.

6. Hoe gebruikt Lookout de gegevens die worden verzameld van mijn mobiele apparaat?

De rechtsgrond voor het gebruik van uw informatie als vermeld in deze Ondernemingsprivacyverklaring is afhankelijk van uw relatie met uw werkgever en de gebruikssituatie van uw werkgever en kan het volgende omvatten: (a) Gebruik van uw persoonsgegevens is noodzakelijk om onze verplichtingen uit te voeren onder een contract met u (bijvoorbeeld voor het uitvoeren van het arbeidscontract door uw werkgever, of voor Lookout 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 de werkgever of 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 dat van uw werkgever 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); en naleving van juridische vereisten, zoals vereisten die passende gegevensbeveiliging vragen.

Met de gegevens die we van uw mobiele apparaat verzamelen, kunnen we dreigingen jegens u en/of uw werkgever detecteren, ons Endpoint Security-product verbeteren en onze andere productaanbiedingen verbeteren. Als we tijdens het analyseren van de applicaties op uw mobiele apparaat een applicatie tegenkomen die we niet eerder hebben geanalyseerd, kunnen we een kopie van een deel of de gehele applicatie downloaden om deze te analyseren en te bepalen of dit een risico vormt. We bieden u de optie de applicatie met beveiligingsrisico te verwijderen, of het risico te negeren. We verzamelen ook uw herstelkeuze voor schadelijke bestanden en applicaties (bijv. verwijderen of negeren) en kunnen ook de verzamelde gegevens gebruiken om de risicodreiging van uw apparaat te categoriseren (bijv. Laag, Gemiddeld, Hoog).

Als ondernemingsproduct verzamelt de Lookout MES de gegevens waarmee niet alleen uw mobiele apparaat wordt beveiligd, maar ook uw werkgever.

We kunnen ook gegevens die zijn verzameld van uw mobiele apparaat combineren met gegevens die zijn verzameld via derde partijen om onze producten te verbeteren, inclusief ons Mobile Endpoint Security-

product. Deze gegevens worden gede-identificeerd. Als de resultaten van onze analyse openbaar worden gedeeld, wordt dit gedaan in samengevoegde en gede-identificeerde vorm om uw privacy en de privacy van uw werkgever te beschermen.

Als onze verwerking van gegevens gebaseerd is op uw toestemming, mag u uw toestemming op ieder moment intrekken, zonder dat dit van invloed is op de wettigheid van de verwerking die is uitgevoerd voor het intrekken van uw toestemming. Neem om uw toestemming in te trekken contact op met uw werkgever (of, waar van toepassing, met ons via onderstaande contactinformatie).

7. Deelt Lookout mijn gegevens met anderen?

Ja. Omdat dit een ondernemingsproduct is, worden bepaalde gegevens gedeeld met uw werkgever, of met anderen die zijn bevoegd door uw werkgever om dergelijke gegevens in te zien. Via het Mobile Endpoint Security-dashboard krijgen werkgevers of hun bevoegde personen toegang tot bepaalde informatie met betrekking tot de veiligheid van uw mobiele apparaat. Uw werkgever kan uw unieke apparaatkenmerken zien, zoals apparaatmodel en provider. Uw werkgever heeft inzicht in applicaties die we hebben geïdentificeerd als schadelijk, alsmede in de applicaties die in overtreding zijn van toepasselijke bedrijfsbeleidsregels van uw werkgever. Neemt u contact op met uw werkgever over hoe dergelijke overtredingen van toepasselijke bedrijfsbeleidsregels op u van invloed kunnen zijn.

Als u het Mobile Endpoint Security-product hebt geïnstalleerd en geactiveerd als onderdeel van een product van een MDM-leverancier, kunnen we gegevens delen van uw mobiele apparaat met die MDM-leverancier.

We kunnen alle gegevens aan u gerelateerd delen met derde partijen, inclusief andere leden van onze groep bedrijven, en serviceleveranciers of partners die we hebben aangetrokken om bedrijfsgerelateerde functies uit te voeren namens ons. Hieronder kunnen serviceleveranciers vallen die: (a) klantenondersteuning, technische of operationele ondersteuning bieden; (b) bestellingen en verzoeken van gebruikers en werkgevers afhandelen; (c) betalingen afhandelen; (d) onze online diensten hosten; (e) databases onderhouden; (f) gegevens analyseren voor productverbetering; en (g) op andere wijze ons Endpoint Security-product of andere producten en diensten van Lookout ondersteunen of op de markt brengen. We kunnen alle gegevens gerelateerd aan u vrijgeven in reactie op een dagvaarding, gerechtelijk bevel of ander juridisch proces dat we ontvangen, of om onze wettelijke rechten vast te stellen of uit te oefenen of om ons te verdedigen tegen een rechtsvordering. Als we een verzoek om informatie ontvangen van een lokale, federale of buitenlandse wetshandhavingsinstelling of staatshandhavingsinstelling, dan proberen we die verzoeken over te dragen aan uw werkgever voor verwerking door de werkgever, maar we behouden ons het recht voor rechtstreeks te reageren en de verzochte informatie te verstrekken waar we een dergelijke reactie wettelijk toepasselijk vinden. We kunnen gegevens over u vrijgeven als we in goed vertrouwen van mening zijn dat dergelijke vrijgave passend is voor het onderzoeken, voorkomen of handelen betreffende mogelijke illegale activiteiten, vermoedelijke fraude, situaties met mogelijke dreigingen voor de fysieke veiligheid van een persoon,

overtredingen van dit privacybeleid, de Licentieovereenkomst of de Eindgebruikersovereenkomst voor het Endpoint Security-product, en/of om de rechten en het eigendom van Lookout, onze werknemers, gebruikers en het publiek te beschermen. Hieronder kan vallen het delen van uw informatie met wetshandhaving, overheidsinstellingen, rechtbanken en/of andere organisaties.

We kunnen gegevens over u delen in relatie tot een fusie, reorganisatie, een verkoop van een deel of alle activa van Lookout, of een financiering of acquisitie van het geheel of een deel van ons bedrijf door een ander bedrijf.

8. Welke informatie kan mijn werkgever NIET zien?

Lookout laat uw werkgever de inhoud van uw persoonlijke e-mail, zoekgeschiedenis, contacten, agenda of persoonlijke sms-berichten niet zien. Uw werkgever kan bepaalde rechten hebben om deze informatie zelf in te zien, waar deze informatie bijvoorbeeld wordt verzonden met behulp van een door de werkgever verstrekt apparaat of netwerk. Lookout geeft uw werkgever echter geen inzicht in applicaties op uw apparaat, tenzij ze een dreiging lijken te bevatten of in overtreding zijn van een bedrijfsbeleidsregel.

9. Gebruikt u mijn gegevens voor marketingdoeleinden?

We verzamelen geen gegevens die van uw mobiele apparaat zijn verzameld door automatische methoden om producten aan u te verkopen en we delen ze ook niet met derde partijen voor marketingdoeleinden. We kunnen informatie die is verzameld van uw apparaat samenvoegen om onderzoek uit te voeren en inzicht te vergaren in de beveiliging en dreigingen van mobiele apparaten. In deze gevallen wordt de samengevoegde informatie in het onderzoek gede-identificeerd.

We kunnen de informatie die u rechtstreeks verstrekt aan ons of aan derde partijen zoals onze partners en marketeers echter gebruiken om u te voorzien van informatie over Lookout en onze producten en diensten, inclusief conferenties en andere evenementen waaraan Lookout kan deelnemen of die Lookout kan organiseren.

10. Hoe beschermt Lookout mijn gegevens en hoe lang worden ze bewaard?

We hebben redelijke administratieve, technische en fysieke beveiligingsmaatregelen geïmplementeerd om te beveiligen tegen onbevoegde toegang, vernietiging of wijziging van uw informatie. Deze veiligheidsmaatregelen zijn gericht op het aanpakken van de gevoeligheid van de informatie die we verzamelen, verwerken en opslaan, alsmede op de huidige status van de technologie.

Hoewel we passende maatregelen treffen om te beschermen tegen onbevoegde vrijgave van informatie, kunnen we, omdat geen enkele verzendmethode via het internet of elektronische opslagmethode 100% veilig is, niet garanderen dat informatie die we verzamelen nooit wordt vrijgegeven op een manier die niet

overeenstemt met deze privacyverklaring.

Het is ons beleid persoonsgegevens slechts zo lang te bewaren als redelijkerwijs nodig voor het verstrekken van producten en diensten aan u en anderen of als anderszins verplicht voor naleving van de wet. We kunnen uw gegevens verwijderen na 90 dagen als uw account inactief is en als anderszins vermeld in onze Servicevoorwaarden. Informatie kan blijven bestaan in kopieën die zijn gemaakt voor back-up- en bedrijfscontinuïteitsdoeleinden. In deze situaties worden alle gegevens beveiligd met 256-bit-versleuteling.

11. Waar bewaart Lookout mijn gegevens?

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 overdracht 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 het e-mailadres of 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 kunnen 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”).

12. Welke rechten en keuzes heb ik omtrent mijn gegevens?

Inwoners van de Europese Unie en bepaalde andere rechtsgebieden kunnen bepaalde rechten hebben om (1) toegang tot of rectificatie of verwijdering van informatie te verzoeken die we over hen verzamelen, (2) een beperking aan te vragen op de verwerking van hun informatie, (3) een bezwaar in te dienen tegen de verwerking van hun informatie of (4) in zeer beperkte gevallen de portabiliteit te verzoeken van bepaalde informatie. Om deze en andere rechten uit te oefenen, neemt u contact op met uw werkgever (of MDM-leverancier, als van toepassing). U kunt ook contact met ons opnemen via onderstaande contactgegevens. Onder passende omstandigheden kunnen we het verzoek doorsturen naar de werkgever en zijn instructies opvolgen voor het afhandelen ervan. Inwoners van Frankrijk en bepaalde andere rechtsgebieden kunnen ook instructies verstrekken betreffende de manier waarop wij uw informatie kunnen blijven bewaren, wissen en delen na uw overlijden en, waar van toepassing, de persoon die u hebt aangewezen voor het uitoefenen van

deze rechten na uw overlijden.

13. Hoe kan ik contact met u opnemen met meer vragen?

Als u nog vragen hebt, raden we u aan u contact op te nemen met uw werkgever (of MDM-leverancier, als van toepassing). U kunt uw vragen ook rechtstreeks richten aan 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. Inwoners van de EU kunnen ons bereiken via een e-mail naar Lookout, Inc., T.a.v.: G.J. Schenk, SVP International Sales, Florapark 3, 2012 HK Haarlem.

Ingangsdatum: 25 mei 2018