
Lookout, Inc.

Lookout for Work-app

Privacyverklaring

Ingangsdatum: 1/1/2020

Creatiedatum: 24/10/2016

Revisiedatum: 1/1/2020

Privacyverklaring Lookout for Work-app

Lookout, Inc. (“Lookout,” “we,” of “ons” of “onze”) is ervan overtuigd dat uw privacy net zo belangrijk is als uw veiligheid, dus we willen volledig transparant zijn over de gegevens die we verzamelen om uw apparaat en de veiligheid van uw werkgever te beschermen. Lookout, Inc. verstrekt u deze Ondernemingsprivacyverklaring (de “Verklaring”) waarin de informatiepraktijken met betrekking tot onze Lookout for Work-app (de “Services”) worden beschreven. Deze Verklaring is van toepassing op de gegevens die van of over u worden verzameld via uw installatie en activering van onze Services op uw mobiele apparaat. Door de Services te downloaden en activeren, geeft u toestemming voor de verzameling, het gebruik, de vrijgave en de opslag van gegevens zoals beschreven in deze Verklaring. Op informatie over u die Lookout op een andere manier verzamelt dan via het gebruik van de Services, is een andere privacyverklaring van toepassing.

Het kan zijn dat u instructies hebt ontvangen voor het downloaden en installeren van de Services in het kader van uw dienstverband bij een organisatie die (1) vereist dat alle of een deel van zijn werknemers de Services installeert of (2) vereist dat alle of een deel van zijn werknemers een Mobile Device Management pakket installeert met daarin de Services. Tenzij uitdrukkelijk anders is aangegeven in deze Verklaring, heeft deze uitsluitend betrekking op onze informatiepraktijken ten aanzien van onze Services. Als u vragen of verzoeken hebt met betrekking tot de praktijken voor het 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 Verklaring op ieder moment aan te passen aan wijzigingen in de wet, onze gegevensverzamelings- en gebruikspraktijken, de kenmerken van de Services of technologische ontwikkelingen. Bij wezenlijke veranderingen in deze Verklaring zullen we trachten u op de hoogte te stellen. Als u bezwaar hebt tegen de informatie in deze Verklaring, dient u te stoppen met uw gebruik van de Services.

In deze Verklaring beantwoorden we enkele algemene vragen over onze Services. Deze Verklaring bevat antwoorden op de volgende vragen:

1. **Wat is de Lookout for Work-app?**
2. **Welke gegevens verzamelt Lookout van uw mobiele apparaat?**
3. **Leest of controleert Lookout mijn e-mails en bekijkt Lookout mijn foto's?**
4. **Verzamelt Lookout andere gegevens over mij buiten mijn mobiele apparaat?**
5. **Wanneer verzamelt Lookout gegevens van mijn mobiele apparaat?**
6. **Hoe gebruikt Lookout de gegevens die worden verzameld van mijn mobiele apparaat?**
7. **Deelt Lookout mijn gegevens met anderen?**
8. **Welke informatie kan mijn Werkgever NIET zien?**
9. **Gebruikt u mijn gegevens voor marketingdoeleinden?**
10. **Hoe beschermt Lookout mijn gegevens en hoe lang worden ze bewaard?**
11. **Waar bewaart Lookout mijn gegevens?**
12. **Welke rechten en keuzes heb ik omtrent mijn gegevens?**
13. **Hoe kan ik contact opnemen als ik meer vragen heb?**

1. **Wat is de Lookout for Work-app?**

De Lookout for Work-app is een mobiele beveiligingsoplossing die mobiele apparaten en bedrijven beschermt tegen dreigingen en overtredingen van het bedrijfsbeleid. Lookout 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).

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:

- **Analytische gegevens** die worden gebruikt voor het analyseren van productprestaties op uw apparaat,
- **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 de app verzamelen,
- **Configuratiegegevens**, zoals of uw apparaat is geconfigureerd voor root-toegang of dat de hardwarebeperkingen van het apparaat zijn verwijderd,
- **Apparaatgegevens**, waaronder de apparaat- en MDM-identifiers van uw mobiele apparaat,
- **Firmwaregegevens/gegevens van het besturingssysteem**, waaronder de fabrikant en het model van uw mobiele apparaat, bepaalde technische instellingen op uw mobiele apparaat (inclusief de schermafmeting van uw mobiele apparaat en de firmwareversie), het type en de versie van het besturingssysteem op uw mobiele apparaat,
- **Identificatiegegevens**, zoals uw werkmailadres, worden optioneel geregistreerd tenzij uw werkgever de functie Privacy Controls in onze Services gebruikt,
- **Netwerkgegevens**, waaronder metadata over netwerken waarmee uw mobiele apparaat verbinding maakt (inclusief maar niet beperkt tot de SSID van het netwerk of het unieke MAC-/BSSID-adres van uw netwerkapparatuur), en het IP-adres (dat uw land en geografische locatie kan aangeven),
- **Webcontentgegevens**, waaronder URL's en domeinen voor schadelijke content en content die aanvullende analyse vereist.

Let erop dat we bepaalde soorten informatie nodig hebben voor het aanbieden van de Services. Als u dergelijke informatie niet aan ons verschaft, of als ons wordt verzocht deze te verwijderen, kan het zijn dat u niet langer toegang hebt tot de Services.

3. Leest of controleert Lookout mijn e-mails en bekijkt Lookout mijn foto's?

Nee. Lookout verzamelt alleen metadata over applicaties op uw apparaat, of de applicatie zelf. 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.

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

Uw Werkgever kan uw e-mailadres aan Lookout verstrekken om de Services te activeren. Als de Services geïntegreerd zijn met een MDM-oplossing en Privacy Controls zijn ingeschakeld, registreert Lookout uw e-mailadres niet.

Als u de Services 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.

5. Wanneer verzamelt Lookout gegevens van mijn mobiele apparaat?

Nadat u de Services hebt gedownload, geïnstalleerd en geactiveerd, begint Lookout onmiddellijk met het verzamelen van gegevens van uw apparaat om te waarborgen dat het vrij is van dreigingen en voldoet aan het bedrijfsbeleid. 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?

We gebruiken de verzamelde gegevens voor diverse zakelijke en commerciële doeleinden. Met de gegevens die we van uw mobiele apparaat verzamelen, kunnen we bijvoorbeeld dreigingen jegens u en/of uw Werkgever detecteren, onze Services verbeteren en onze andere productaanbiedingen verbeteren. Ook kunnen we gegevens die zijn verzameld van uw mobiele apparaat combineren met gegevens die zijn verzameld van derden om onze Services te verbeteren. Deze gegevens worden gepseudonimiseerd. Als de resultaten van onze analyse openbaar worden gemaakt, gebeurt dit in samengevoegde en gepseudonimiseerde vorm om uw privacy en de privacy van uw Werkgever te beschermen. Hoe we uw informatie gebruiken, is afhankelijk van het type gegevens zoals hieronder uitgelegd:

- **Applicatiegegevens.** We gebruiken deze gegevens om onze Services te verlenen door scans van applicatiebestanden uit te voeren, met als doel vast te stellen of applicaties schadelijk gedrag vertonen. 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, afhankelijk van de manier waarop uw Werkgever de Services heeft geconfigureerd. Zoals uitgelegd in artikel 3 verzamelen we geen gebruikersgegevens die u in de applicaties invoert wanneer u een exemplaar van de applicatie downloadt.
- **Configuratiegegevens.** We analyseren configuratiegegevens over uw apparaat om vast te stellen of uw apparaat is gewijzigd, aangetast of onveilig is geconfigureerd, bijvoorbeeld doordat het is geïnfecteerd, doordat er rooting of jailbreaking op is toegepast of doordat er geen beveiligingscode is ingesteld.
- **Apparaatgegevens.** We gebruiken apparaat- of MDM-identifiers om uw apparaat te koppelen aan een apparaat in een systeem van een derde, zoals een Mobile Device Management-oplossing, zodat we aan dat systeem kunnen rapporteren of uw apparaat dreigingen is tegengekomen.
- **Firmwaregegevens/gegevens van het besturingssysteem.** Lookout gebruikt deze informatie om aantasting van firmware en besturingssystemen te herkennen en u te informeren als er een beveiligingsupdate beschikbaar is voor uw apparaat.
- **Identificatiegegevens.** We kunnen optioneel uw werkmailadres registreren om contextuele informatie te kunnen verstrekken wanneer we uw Werkgever inlichten over dreigingen die u tegenkomt. We sturen u nooit e-mails zonder toestemming.
- **Netwerkgegevens.** Aanvallers kunnen internetverbindingen, waaronder wifi, gebruiken om gegevens te stelen. Dit staat bekend als een man-in-the-middle-aanval (MitM). We kunnen de SSID gebruiken om deze MitM-aanvallen te identificeren. Lookout kan ook vaststellen in welk land en welke regio u woont aan de hand van uw IP-adres, maar de werkelijke locatiegegevens van het apparaat van de gebruiker (GPS-gegevens) worden niet door Lookout gelezen, opgeslagen of overgedragen. We pseudonimiseren gegevens en voegen deze samen om de populariteit van toepassingen per regio vast te stellen en onze mobiele dreigingsanalyse uit te voeren. Deze informatie blijft gepseudonimiseerd om de privacy van gegevens te waarborgen.
- **Webcontentgegevens.** Lookout gebruikt een VPN-interface om verkeer op uw apparaat te analyseren op dreigingen als onderdeel van onze Safe Browsing-functie, die de toegang tot schadelijke en phishingwebsites blokkeert. De inhoud en geschiedenis van uw verkeer worden niet gedeeld met uw Werkgever en uw Werkgever wordt uitsluitend op de hoogte gesteld als u een dreiging bent tegengekomen.

In overeenstemming met de Algemene Verordening Gegevensbescherming is de rechtsgrond voor het gebruik van uw informatie, zoals beschreven in deze Verklaring, afhankelijk van uw relatie met uw Werkgever en de gebruikssituatie van uw Werkgever en kan het volgende omvatten: (a) gebruik van uw persoonsgegevens dat noodzakelijk is om onze verplichtingen na te komen op grond van een contract met u (bijvoorbeeld voor het uitvoeren van het arbeidscontract door uw Werkgever, of zodat Lookout zich kan houden aan de Servicevoorwaarden die u accepteert door onze apps te downloaden en gebruiken); of (b) gebruik van uw informatie dat niet nodig is voor het uitvoeren van een contract, maar wel voor onze gerechtvaardigde belangen of de gerechtvaardigde belangen van de Werkgever of anderen (bijvoorbeeld om te zorgen voor de beveiliging van de Services, het uitvoeren van de Services, 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 Services leveren); en naleving van juridische vereisten, zoals vereisten die passende gegevensbeveiliging vergen.

7. Deelt Lookout mijn gegevens met anderen?

Aangezien dit een bedrijfsproduct is, worden bepaalde gegevens gedeeld met uw Werkgever of met anderen die door uw Werkgever zijn gemachtigd om dergelijke gegevens in te zien. Via het Services-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 kan inzicht hebben in applicaties die we hebben geïdentificeerd als schadelijk en in applicaties die het toepasselijk bedrijfsbeleid van uw Werkgever schenden. Neem contact op met uw Werkgever voor informatie over de gevolgen die overtredingen van toepasselijk bedrijfsbeleid voor u hebben.

Als u onze Services hebt geïnstalleerd en geactiveerd als onderdeel van een product van een MDM-leverancier, kunnen we de beveiligings- en activeringsstatus van uw mobiele apparaat delen met die MDM-leverancier.

We kunnen alle aan u gerelateerde gegevens delen met derde partijen, waaronder andere leden van onze bedrijvengroep en dienstverleners of partners die we hebben aangetrokken om bedrijfsgerelateerde functies uit te voeren namens ons. Hieronder kunnen dienstverleners vallen die: (a) klantenondersteuning, technische of operationele ondersteuning bieden; (b) bestellingen en verzoeken van gebruikers en Werkgevers afhandelen; (c) onze Services hosten; (d) databases onderhouden; (e) gegevens analyseren voor productverbetering; en (f) op andere wijze onze Services of andere producten van Lookout ondersteunen of op de markt brengen. We kunnen alle aan u gerelateerde gegevens 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 wetshandhavinginstelling of staatshandhavinginstelling, 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 wanneer 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 ondernemen van actie betreffende mogelijke illegale activiteiten, vermoedelijke fraude, situaties met mogelijke dreigingen voor de fysieke veiligheid van een persoon, overtredingen van deze Verklaring, de [Licentieovereenkomst](#) of de [Eindgebruikersovereenkomst](#) voor de Services en/of om de rechten en het eigendom van Lookout, onze werknemers, gebruikers en het publiek te beschermen. Dit kan betekenen dat uw informatie wordt gedeeld met wetshandhavers, overheidsinstellingen, rechtbanken en/of andere organisaties.

We kunnen gegevens over u delen in het kader van 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 deelt alleen informatie met uw Werkgever die uw Werkgever nodig heeft om te waarborgen dat uw apparaat vrij is van dreigingen en in overeenstemming is met het beveiligingsbeleid van het bedrijf. Lookout verleent uw Werkgever bijvoorbeeld geen toegang tot de inhoud van uw e-mail, zoekgeschiedenis, contacten, agenda,

tekstberichten, niet-schadelijke apps die u hebt geïnstalleerd of uw locatie.

9. Gebruikt u mijn gegevens voor marketingdoeleinden?

Gegevens die automatisch van uw mobiele apparaten zijn verzameld, worden niet door ons gebruikt om producten aan u te verkopen en we delen ze niet met derden voor hun marketingdoeleinden. We kunnen informatie die is verzameld van uw apparaat samenvoegen om onderzoek uit te voeren en inzicht te verschaffen in de beveiliging en dreigingen van mobiele apparaten. In deze gevallen wordt de samengevoegde informatie in het onderzoek gepseudonimiseerd.

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

We hebben redelijke administratieve, technische en fysieke beveiligingsmaatregelen geïmplementeerd ter bescherming tegen ongevoegde toegang, vernietiging of wijziging van uw informatie. Deze veiligheidsmaatregelen zijn afgestemd op de gevoeligheid van de informatie die we verzamelen, verwerken en opslaan, alsmede op de huidige status van de technologie.

Hoewel we passende maatregelen treffen ter bescherming tegen ongevoegde 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 Verklaring.

Het is ons beleid persoonsgegevens slechts zo lang te bewaren als redelijkerwijs nodig is om onze Services aan te bieden aan u en anderen of voor zover anderszins verplicht om de wet na te leven. We kunnen uw gegevens na 60 dagen verwijderen als uw account inactief is of zoals anders bepaald 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 Services 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. 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.

Als u vragen of klachten hebt over de privacypraktijken van Lookout, inclusief vragen betreffende het Privacyschild, 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.

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

Als u een inwoner van de Europese Economische Ruimte ("EER") bent, hebt u mogelijk de volgende rechten

overeenkomstig de Algemene Verordening Gegevensbescherming (“AVG”):

- **Toegang.** U hebt het recht 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;
- **Rectificatie.** U hebt het recht om correctie te eisen van fouten (onvolledigheid of onjuistheid) in de Persoonsgegevens die we over u bezitten;
- **Verwijdering.** U hebt het recht 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);
- **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;
- **Bezwaar.** U hebt het recht 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.
- **Beperking.** U hebt het recht te eisen dat we onze verwerking van uw Persoonsgegevens in bepaalde omstandigheden beperken, bijvoorbeeld wanneer u de juistheid van die Persoonsgegevens betwist;
- **Intrekking van toestemming.** Als we vertrouwen op uw toestemming (of uitdrukkelijke toestemming) als rechtsgrondslag voor de verwerking van uw Persoonsgegevens, hebt u het recht die toestemming op elk moment in te trekken.

Neem contact op met uw Werkgever als u deze rechten wilt uitoefenen. Wanneer Lookout optreedt als verwerkingsverantwoordelijke, kunt u ook contact met ons opnemen om deze rechten uit te oefenen. U vindt onze contactgegevens hieronder. Onder passende omstandigheden kunnen we het verzoek doorsturen naar de Werkgever en zijn instructies opvolgen voor het afhandelen ervan. We reageren tijdig en uiterlijk binnen 30 dagen op uw verzoek. Echter, Lookout is in bepaalde situaties mogelijk niet in staat om toegang te verschaffen tot de Persoonsgegevens die we over u bezitten of al deze Persoonsgegevens te verwijderen.

Als u een inwoner bent van de EER 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 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. Inwoners van de Europese Unie kunnen 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.

U hebt mogelijk bepaalde rechten op grond van de toepasselijke wet, waaronder de Algemene Verordening Gegevensbescherming. Neem contact op met uw Werkgever als u enige van deze rechten wilt uitoefenen. U kunt ook contact met ons opnemen via onderstaande contactgegevens.

13. Hoe kan ik contact opnemen als ik meer vragen heb?

Als u nog vragen hebt, raden we u aan u contact op te nemen met uw Werkgever. U kunt uw vragen ook rechtstreeks richten aan onze Functionaris Gegevensbescherming via het e-mailadres privacy@lookout.com of door een schrijven te sturen naar Lookout, Inc., T.a.v.: Michael Musi, Data Protection Officer, 28 State Street, 19th Floor, Boston, MA 02109, Verenigde Staten. Inwoners van de EER kunnen ons bereiken door een e-mail te sturen naar Lookout, Inc., T.a.v.: G.J. Schenk, SVP International Sales, Florapark 3, 2012 HK Haarlem.