



Politique de confidentialité de Lookout Personal

Date de création : 15/11/2016

Date de révision : 22/05/2018

État : Approuvé

Le présent document, ainsi que les informations qu'il contient sont la propriété exclusive de Lookout, Inc. et sont confidentiels. Sauf accord écrit exprès de Lookout, Inc., il est interdit de copier, de reproduire ou de divulguer toute partie du présent document à des tierces parties.

Produits proposés dans l'application Lookout Personal	7
1. Nous recueillons des informations à votre sujet pour vous délivrer les services Lookout	7
2. Informations recueillies par Lookout pour l'application Lookout Basic Personal	8
a. Informations d'inscription	8
b. Informations relatives à l'appareil	8
c. Informations de localisation	9
d. Adresses URL	9
3. Fonctionnalités proposées dans l'application Lookout Personal	9
a. Sécurité	9
b. Appareil perdu	10
c. Sauvegarde (Contacts)	10
d. Prise en charge de plusieurs appareils	10
4. Informations recueillies par Lookout pour nos services Premium dans l'application Personal	11
a. Informations recueillies lors de la mise à niveau vers un service Premium	11
b. Informations relatives au paiement	11
c. Recueil de données relatives à l'alerte de vol	11
d. Navigation sécurisée	12
5. Fonctionnalités offertes dans le cadre du service Premium Lookout	12
a. Appareil perdu	12
b. Alerte de vol	12
c. Sauvegarde (journaux d'appel et photos)	13
d. Navigation sécurisée	13
e. Wi-Fi sécurisé	13

f. Breach Report (disponible en anglais uniquement)	13
g. Désactivation des fonctionnalités	13
6. Informations recueillies à l'aide de Lookout Premium Plus (États-Unis uniquement)	13
7. Fonctionnalités fournies avec Premium Plus (États-Unis uniquement)	14
1. Identity Monitoring	14
a. Cybersurveillance	15
b. Surveillance des réseaux sociaux	15
c. Surveillance NSS	15
2. Assurance et récupération	15
a. Assurance contre le vol d'identité	15
b. Assistance à la récupération	15
c. Récupération de portefeuille perdu	15
9. Analyse des données - Comment nous utilisons les informations recueillies à partir de votre appareil de point de terminaison mobile	16
10. Votre utilisation du site Web de Lookout et du site Web mobile et les informations recueillies	17
a. Contenu et promotions	17
b. Fonctionnalités de réseaux sociaux	17
11. Politique relative aux cookies du site Web de Lookout	18
12. Base légale de l'utilisation de vos informations	19
a. Nous utilisons vos informations pour fournir, améliorer et promouvoir nos services	20
b. Nous pouvons divulguer vos informations conformément à la législation	20
c. Nous partageons vos informations afin de fournir ou d'améliorer nos services	21
13. Vos données peuvent être incluses à des rapports de sécurité	21
14. Vos choix	22
a. Vous pouvez accéder à vos paramètres et les mettre à jour	22
b. Désabonnement aux e-mails	22

c. Publicités personnalisées	22
d. Localisation	23
15. Politique de conservation des données	23
16. Les informations publiées sur notre blog et notre forum communautaire sont publiques	23
17. Nous prenons la sécurité au sérieux	23
18. Vous êtes responsable de l'exactitude et de la confidentialité de votre adresse électronique et de votre mot de passe	24
19. Avis aux utilisateurs californiens	24
20. Visiteurs internationaux, Privacy Shield et RGPD	25
21. Utilisateurs de moins de 16 ans	27
22. Nous ne sommes pas responsables du contenu des sites Web tiers	27
23. Changement de contrôle	27
24. Toute modification de cette politique fait l'objet d'un avis sur notre site Web	27
25. Contactez-nous pour toute question ou préoccupation	28

Historique de révision

Lookout, Inc. contrôle le présent document ; par conséquent, toute impression dudit document constitue une copie de « référence ». Les utilisateurs ont la charge de s'assurer qu'ils disposent de la version à jour. Dès lors qu'une partie du présent document doit être une mise à jour, l'intégralité du document est révisée.

Communiqué de presse	Date	Description	Envoyé par
1.0	22/09/2016	Première ébauche	Marcelo Guerra
2.0	26/09/2017	Mise à jour	Joseph Leung
3.0	01/04/2018	Mise à jour visant à traduire les changements apportés au produit et à décrire les modifications de la réglementation. Déplacement des détails de l'historique du document à la fin du document.	Kimberly Snow

Date d'entrée en vigueur : 25 mai 2018

Le présent document est notre Politique de confidentialité, qui explique quelles sont les informations que nous recueillons et comment nous les utilisons. Nous vous recommandons de lire la Politique de confidentialité, ainsi que les [Conditions d'utilisation](#) de Lookout (disponibles sur www.lookout.com/legal/terms), car les deux documents concernent votre utilisation de l'application Lookout Personal. Notre Politique de confidentialité s'applique à nos sites Web et à nos sites Web pour mobile, y compris sur www.lookout.com, à notre application Lookout Personal et à tous les autres services Lookout fournis dans le cadre de l'application Lookout Personal (tels que définis dans nos [Conditions d'utilisation](#)).

La politique de confidentialité du produit Lookout Enterprise Mobile Endpoint Security est décrite dans la Déclaration de confidentialité entreprise de Lookout.

La présente Politique de confidentialité décrit le recueil et l'utilisation de données à caractère personnel (DP). Parmi les données à caractère personnel (DP) recueillies auprès de vous figurent votre nom, votre adresse électronique, votre numéro de téléphone et/ou l'identifiant unique de votre appareil mobile. Le terme Données à caractère personnel couvre également les informations personnellement identifiables et les données à caractère personnel, telles que définies dans le RGPD ou Règlement général sur la protection des données (règlement (UE) 2016/679) (« RGPD »).

Lookout se réserve le droit de modifier la présente Politique de confidentialité suivant l'évolution de la législation, de nos pratiques de collecte et d'utilisation des données, des fonctionnalités de nos services ou des technologies. Veuillez consulter régulièrement ce document ou les pages Web de Lookout.com afin de prendre connaissance des dernières modifications. En continuant d'utiliser nos services, vous acceptez ces modifications et consentez à être lié(e) par la politique mise à jour. Si vous avez des questions concernant la présente Politique de confidentialité, veuillez nous contacter à l'adresse privacy@lookout.com. Vous pouvez accéder à la présente politique à partir de l'écran de connexion de l'application mobile Lookout, des paramètres de l'application Lookout Personal, ainsi que sur le site Web de notre société.

Produits proposés dans l'application Lookout Personal

Lookout propose différents niveaux au sein de l'application Lookout Personal. Chaque niveau permet d'accéder à certaines fonctionnalités de sécurité de Lookout. Les informations requises pour bénéficier de ces services peuvent varier et sont répertoriées dans le présent document afin de vous permettre de comprendre quelles informations nous recueillons directement auprès de vous, à partir de votre appareil et comment nous utilisons ces informations. Pour en savoir plus sur les fonctionnalités des produits dédiés à l'application Lookout Personal pour les appareils iOS et Android, rendez-vous ici

<https://www.lookout.com/products/personal/ios> et <https://www.lookout.com/products/personal/android>.

1. Nous recueillons des informations à votre sujet pour vous délivrer les services

Lookout

Sauf indication contraire, lorsque nous recueillons vos informations, nous les stockons en les associant à votre compte. Nous prenons le respect de la vie privée très au sérieux. C'est pourquoi nous nous engageons à utiliser et à divulguer ces informations uniquement de la façon décrite dans la présente Politique de confidentialité.

Certains de nos produits sont autonomes et ne recueillent qu'une quantité limitée d'informations, voire aucune. La disponibilité des fonctionnalités varie d'un produit et d'un pays à l'autre. Tous les articles de la présente Politique de confidentialité ne s'appliquent donc pas à ces produits.

Veillez noter que nous avons besoin de certains types d'informations afin de vous permettre d'accéder aux services Lookout. Si vous refusez de nous fournir ces informations ou que vous nous demandez de les supprimer, vous risquez de ne plus pouvoir accéder aux services Lookout.

Veillez noter que le recueil des données des applications et des analyses de sécurité a pour vocation de vous protéger, vous et vos données. Le recueil de ces données permet également d'optimiser et d'améliorer nos services Lookout.

Lookout recueille des données concernant votre appareil, y compris la marque, le modèle, le type de système d'exploitation et sa version, ainsi que les applications déjà installées. Ces données sont rendues anonymes et associées aux données anonymisées d'autres clients pour connaître la popularité des appareils dans les applications par région. Ces données restent anonymes pour garantir la confidentialité des données à caractère personnel. L'association de données client de manière sûre et confidentielle permet à Lookout de mieux appréhender les menaces de sécurité actuelles. Elle permet également d'améliorer les services et les fonctionnalités de sécurité de Lookout. Nous sommes, en outre, susceptible de rendre public des comptes

rendus élaborés à partir de ces données agrégées et anonymisées afin de faciliter la compréhension des menaces mobiles et du comportement de certaines applications mobiles.

2. Informations recueillies par Lookout pour l'application Lookout Basic Personal

a. Informations d'inscription

Afin de créer un compte, vous devez indiquer votre adresse électronique, ainsi qu'un mot de passe.

b. Informations relatives à l'appareil

Lorsque vous utilisez les services Lookout, nos serveurs enregistrent certaines informations relatives à votre appareil mobile. Il peut s'agir de l'identifiant du matériel (par ex. : IMEI), de l'identifiant de l'abonné (par ex. : IMSI), du nom de l'appareil, du numéro de téléphone mobile, du type et du fabricant de l'appareil, du type et de la version du système d'exploitation, de l'opérateur, du type de réseau, du pays d'origine, de l'adresse IP et des dates et heures de vos requêtes. Nous recueillons également des informations relatives aux applications présentes sur votre appareil afin d'exécuter des analyses et de télécharger des copies des fichiers d'application analysés. Nous pouvons notamment télécharger une copie de tout ou partie des fichiers d'application que nous analysons pour la première fois. Nous sommes aussi susceptibles de recueillir des informations relatives au comportement des applications sur votre appareil (par ex. : si une application envoie des SMS surfacturés qui peuvent être ajoutés à votre facture de téléphone) et aux services réseau avec lesquels les applications communiquent, le but étant de déceler les activités malveillantes (par ex. : si une application communique avec un serveur connu pour sa propension à héberger des sites Web de phishing). À chaque analyse, nous recueillons des informations qui décrivent les fichiers d'application reconnus comme étant potentiellement indésirables. Lookout propose ensuite des recommandations de correction pour ces fichiers (par ex. : désinstaller ou ignorer).

Nous utilisons les informations susmentionnées pour vous fournir nos services, ainsi qu'une assistance si nécessaire. Nous agrégeons des informations concernant l'analyse des menaces mobiles. Les informations ainsi agrégées sont rendues anonymes pour empêcher l'identification d'un individu.

Pour en savoir plus sur l'analyse des menaces mobiles de Lookout, rendez-vous sur <https://www.lookout.com/why-lookout>.

c. Informations de localisation

Certaines des fonctionnalités que nous proposons sont plus efficaces si nous pouvons localiser votre appareil mobile. Avec votre accord, que vous nous donnez lors de la première inscription, Lookout peut recueillir des informations de localisation de deux manières : soit directement sur votre appareil mobile, soit (dans certains cas) grâce aux données envoyées par une antenne relais ou un point d'accès Wi-Fi. Nous pouvons faire appel à des prestataires de services tiers pour convertir ces données en informations de localisation exploitables. Afin d'empêcher tout partage des données de localisation, accédez aux paramètres de votre appareil mobile et désactivez les services de localisation.

d. Adresses URL

Afin de vous fournir le service Safe Browsing, nous pouvons transmettre les URL que vous recevez ou consultez sur votre téléphone à un service Lookout ou tiers pour déterminer si elles sont dangereuses (par ex. : si elles contiennent des dispositifs de phishing, des logiciels malveillants ou des exploits). Si nous déterminons que l'URL consultée est dangereuse, nous stockons un enregistrement de celle-ci. Nous utilisons l'enregistrement des URL dangereuses que vous consultez (1) pour vous avertir que vous avez tenté d'accéder à un site dangereux (par ex. : lorsque vous vous connectez au site Web de Lookout ou par e-mail) et (2) pour améliorer notre produit et réaliser des analyses. Si vous ne souhaitez pas que nous enregistrons les URL dangereuses que vous consultez, désactivez la fonction Safe Browsing. Toutes les autres fonctionnalités Lookout continueront de fonctionner normalement.

3. Fonctionnalités proposées dans l'application Lookout Personal

a. Sécurité

Disponibles sur différentes plates-formes, les fonctionnalités de sécurité de Lookout protègent votre appareil contre les menaces de cybersécurité. Les informations requises pour exécuter ces fonctionnalités sont recueillies lorsque vous utilisez l'application Lookout. Pour en savoir plus sur ces informations, reportez-vous à l'article Informations relatives à l'appareil du présent document.

Les fonctionnalités de sécurité de Lookout, qui varient d'une plate-forme à une autre, assurent la sécurité de votre appareil de différents moyens, tels que la recherche d'applications et de fichiers malveillants et la détection d'un système d'exploitation obsolète. Pour en savoir plus sur la technologie de sécurité prédictive de Lookout, rendez-vous sur www.lookout.com. Des analyses automatiques de votre appareil peuvent être effectuées à intervalles réguliers pour recueillir des informations sur les fichiers d'applications, d'appareil et de système d'exploitation présents sur votre appareil. Lookout réunit les résultats des analyses effectuées par

nos services et des dispositions de sécurité les plus récentes de l'appareil. En outre, des mises à jour régulières des définitions des menaces sont effectuées. Ces activités permettent de protéger votre point de terminaison mobile en autorisant l'application Lookout à détecter et à répondre aux menaces sur votre appareil mobile. Vous pouvez activer ou désactiver cette fonctionnalité dans les paramètres de l'application Lookout.

b. Appareil perdu

Les fonctionnalités Theft Protection de Lookout comprennent des capacités Missing Device, telles que Locate et Scream qui fonctionnent à distance à partir de votre compte personnel sur lookout.com. La fonctionnalité Signal Flare vous permet ainsi de connaître la dernière position connue de votre téléphone si jamais vous le perdez et que sa batterie se décharge complètement. Lorsque vous activez Signal Flare, cette dernière recueille des informations de localisation et les envoie à Lookout dès que votre batterie est faible. Nous enregistrons la position de votre téléphone lorsque nous recevons l'alerte de batterie faible sur Lookout.com. Vous pouvez activer ou désactiver cette fonctionnalité dans les paramètres de l'application Lookout.

Lorsque vous activez les fonctionnalités Missing Device, votre navigateur envoie des informations de localisation à des fournisseurs de cartes tiers (par ex. : Google Maps) afin d'afficher une carte indiquant cette position sur votre compte personnel Lookout. Lors de l'activation de cette fonctionnalité, nous suivons la position de l'appareil pendant plusieurs minutes afin de vous indiquer sa position exacte. Vous pouvez supprimer ces informations, conservées dans l'historique de votre compte, à tout moment à partir des paramètres de votre compte. Si vous choisissez de supprimer ces informations ou de désactiver votre compte, Lookout rend ces données anonymes afin d'empêcher leur association à vos données à caractère personnel.

c. Sauvegarde (Contacts)

La fonctionnalité Backup de Lookout permet aux utilisateurs de sauvegarder leurs contacts. Ces informations sont envoyées aux serveurs à l'aide d'un protocole chiffré et stockées dans le cloud de Lookout. Vous pouvez accéder à ces informations ou les supprimer à partir de votre compte sur Lookout.com. Vous pouvez activer ou désactiver cette fonctionnalité dans les paramètres de l'application Lookout.

d. Prise en charge de plusieurs appareils

La fonctionnalité Multiple Device Support permet de relier plusieurs appareils à un seul compte principal qui contrôle l'appareil du propriétaire du compte maître, ainsi que certaines fonctionnalités des autres appareils associés. Les propriétaires du compte maître contrôlent certaines fonctions des appareils supplémentaires. Par exemple, dans un compte associé à plusieurs appareils, un utilisateur peut localiser ou accéder aux données de sauvegarde sur n'importe quel appareil relié à ce compte.

4. Informations recueillies par Lookout pour nos services Premium dans l'application Personal

a. Informations recueillies lors de la mise à niveau vers un service Premium

Lookout recueille les mêmes informations que celles nécessaires dans l'application Lookout Basic Personal, à savoir les informations d'inscription, les informations relatives à l'appareil et les informations de localisation (si nécessaire). Outre ces informations, Lookout recueille des données relatives au paiement pour vous permettre d'accéder aux fonctionnalités Premium.

b. Informations relatives au paiement

Si vous souscrivez un abonnement à un service Lookout Premium ou Premium Plus directement auprès de nous, nous faisons appel à un organisme de paiement tiers pour recueillir les informations relatives à votre carte de crédit, y compris le numéro, la date d'expiration et le code de sécurité de votre carte de crédit, ainsi que d'autres informations de facturation nécessaires. Notre prestataire de services tiers utilisera ces informations à des fins de facturation. Lookout recevra des informations concernant votre compte Premium et/ou Premium Plus. Parmi ces informations figureront le montant payé et le moyen de paiement. Les informations relatives à votre carte de crédit et vos coordonnées bancaires ne nous seront pas communiquées et seront conservées par l'organisme de paiement.

Si vous achetez l'application Lookout dans une App Store ou par le biais de votre opérateur, les informations relatives au paiement seront traitées par l'App Store ou l'opérateur. Le paiement n'est pas sous la responsabilité de Lookout. Votre paiement est susceptible d'être traité de différentes façons. Lookout a établi des accords contractuels avec nos partenaires pour s'assurer que vous bénéficiez des performances d'application mobile Lookout attendues. Afin de vous délivrer nos services, l'App Store envoie une confirmation d'achat à Lookout. Les opérateurs peuvent partager votre numéro de téléphone, votre identifiant d'abonné, l'UGS ou toute autre information non financière. L'App Store et votre opérateur ne partageront pas les informations relatives à votre carte de crédit ni les données de facturation. Pour en savoir plus, veuillez vous reporter aux procédures et politiques de traitement des paiements de votre App Store ou de votre opérateur.

c. Recueil de données relatives à l'alerte de vol

Lorsque la fonctionnalité Theft Alert est activée, une photo est prise. La photo et les données de localisation (localisation GPS) sont brièvement stockées sur nos serveurs, le temps de vous les envoyer par e-mail avec une

carte indiquant la position de votre appareil. La photo est ensuite supprimée de notre serveur. Nous envoyons cet e-mail à l'adresse associée à votre compte. Par conséquent, n'oubliez pas de mettre à jour votre adresse électronique dans les paramètres de votre compte. Nous utilisons les informations relatives aux activités de Theft Alert sur votre appareil afin d'étudier, d'optimiser et de dépanner nos produits.

d. Navigation sécurisée

Safe Browsing est une fonctionnalité conçue pour détecter et signaler les URL dangereuses afin de vous offrir la possibilité de les éviter. Cette fonctionnalité est disponible lorsque vous autorisez l'application à exécuter un VPN local. Grâce au VPN, la fonctionnalité Safe Browsing analyse les URL auxquelles le navigateur et les applications souhaitent accéder. Les URL visitées sont rendues anonymes et transmises au cloud de Lookout pour effectuer des contrôles de sécurité. Les chemins des URL sont les seules données associées à votre activité de navigation qui sont envoyées à Lookout. Lookout ne recueille pas votre historique de navigation ni aucune autre information personnelle.

5. Fonctionnalités offertes dans le cadre du service Premium Lookout

Outre les fonctionnalités de base décrites ci-dessus, les clients Premium de Lookout ont accès à de nouvelles fonctionnalités et améliorations.

a. Appareil perdu

Les clients Premium de Lookout bénéficient de capacités supplémentaires dans la fonctionnalité Missing Device. Ils peuvent verrouiller et effacer les données de l'appareil à distance à partir de leur compte personnel sur lookout.com.

b. Alerte de vol

Theft Alert est une fonctionnalité Premium au sein de Theft Protection. Elle vous permet de localiser votre téléphone en cas de perte. Lorsque ces fonctionnalités sont activées, un e-mail vous est envoyé en cas d'événement (par ex. : activation du mode Avion) en relation avec la position de votre appareil. Sur les appareils Android, l'e-mail inclut une photo de la personne, qui est susceptible d'avoir commis le vol, prise à l'aide de l'appareil photo de l'appareil, accompagnée d'informations de localisation afin de vous aider à savoir où (et entre quelles mains) il se trouve en cas de perte ou de vol.

Vous pouvez connaître la position de votre appareil en vous connectant à votre compte sur Lookout.com. Ces fonctionnalités utilisent les données de localisation de votre appareil, votre adresse électronique et votre numéro de téléphone que vous avez transmis à Lookout à partir de l'appareil et vous aident à retrouver votre

téléphone en cas de perte.

c. Sauvegarde (journaux d'appel et photos)

Une fonctionnalité de sauvegarde des journaux d'appel et des photos est proposée aux clients Premium. Vous pouvez accéder à vos photos par le biais de votre compte personnel sur Lookout.com. Vous pouvez supprimer vos photos et les données sauvegardées de votre compte Lookout à tout moment.

d. Navigation sécurisée

Safe Browsing est une fonctionnalité conçue pour détecter et signaler les URL dangereuses afin de vous offrir la possibilité de les éviter. Cette fonctionnalité est disponible lorsque vous autorisez l'application à exécuter un VPN local. Grâce au VPN, la fonctionnalité Safe Browsing analyse les URL auxquelles le navigateur et les applications souhaitent accéder. Les URL visitées sont rendues anonymes et transmises au cloud de Lookout pour effectuer des contrôles de sécurité. Les chemins des URL sont les seules données associées à votre activité de navigation qui sont envoyées à Lookout. Lookout ne recueille pas votre historique de navigation ni aucune autre information personnelle.

e. Wi-Fi sécurisé

La fonctionnalité Safe Wi-Fi permet d'analyser votre connexion Wi-Fi à la recherche d'activités inhabituelles indiquant la dangerosité du réseau ou son attaque en vue de vous alerter. Cette fonctionnalité permet d'empêcher aux pirates d'accéder à vos données à caractère personnel sur le point de terminaison mobile.

f. Breach Report (disponible en anglais uniquement)

La fonctionnalité Breach Report vous alerte en cas de faille et vous recommande des mesures simples et claires à prendre pour vous protéger. Vous pouvez personnaliser les alertes en fonction du type d'entreprise ou de secteur afin de recevoir des recommandations adaptées pour protéger vos données et votre identité.

g. Désactivation des fonctionnalités

Vous pouvez désactiver les fonctionnalités à votre guise en accédant aux paramètres de Lookout. En cas de question ou de problème, veuillez contacter support@lookout.com.

6. Informations recueillies à l'aide de Lookout Premium Plus (États-Unis uniquement)

Les informations recueillies dépendent des types de produits de protection d'identité Premium Plus auxquels vous vous abonnez. Nous avons besoin de ces informations pour vérifier votre identité, vous fournir les

services de protection d'identité et vous facturer les frais convenus. Nous devons communiquer vos informations à des tierces parties (telles que des sociétés de vérification d'identité, agences de renseignements sur les consommateurs, agences d'évaluation du crédit, sociétés de validation des paiements, forces de l'ordre, etc.) afin de vous fournir ces services. Nous sommes susceptibles de transmettre ces informations aux prestataires de services tiers qui nous aident à vous offrir des services de protection d'identité ou les autoriser à recueillir directement certaines informations auprès de vous. Ces prestataires peuvent à leur tour transmettre vos données à des tiers afin de vous fournir les services demandés. Nos prestataires de services et/ou nous-mêmes pouvons également offrir des services de surveillance et d'alerte et obtenir des informations et des rapports qui vous concernent (ou qui concernent les autres personnes que vous avez inscrites) afin de fournir les services de protection d'identité, y compris des rapports sur l'historique des adresses, les noms, les alias, etc. Nous demandons à nos prestataires de services d'utiliser les données recueillies aux seules fins de fournir des services par le biais de l'abonnement Premium Plus à l'application Lookout. Si vous mettez votre abonnement à niveau vers Premium Plus, qui comprend l'assurance contre le vol d'identité, nous utiliserons vos informations pour vous fournir une assistance et la couverture d'assurance applicable dans le cas où votre identité serait compromise.

Si vous optez pour un abonnement Premium Plus, l'application Lookout est susceptible de vous demander vos coordonnées (par ex. : votre nom, adresse, numéro de téléphone et adresse électronique) ; des informations d'ordre privé (numéro de permis de conduire, de sécurité sociale, de passeport ou autre numéro d'identification) ; des informations financières (par ex. : numéros de compte bancaire et de carte de crédit/débit) ; votre numéro d'assurance maladie et d'autres informations personnelles à votre sujet (ou au sujet des autres personnes que vous inscrivez à ce service). Pour en savoir plus ou vous tenir informé(e), rendez-vous à la [section Produit](#) sur Lookout.com.

7. Fonctionnalités fournies avec Premium Plus (États-Unis uniquement)

Outre les fonctionnalités de base (Missing Device, Security and Backup) et les fonctionnalités Premium (Theft Alerts, Safe Wi-fi, Breach Report, Photo Backup), les utilisateurs Premium Plus bénéficient d'une protection d'identité, qui comprend les fonctionnalités Identity Monitoring, Identity Insurance and Restoration.

1. Identity Monitoring

En optant pour Lookout Premium Plus, vous bénéficierez de services pour vous aider à protéger votre identité et vos informations personnelles.

a. Cybersurveillance

La fonctionnalité Cyber Watch passe internet au crible à la recherche d'informations privées à votre sujet et propose des alertes et des mesures recommandées en cas d'exposition de vos informations personnelles.

b. Surveillance des réseaux sociaux

La fonctionnalité Social Media Watch contrôle la confidentialité de vos informations personnelles sur les réseaux sociaux et vous envoie des alertes en cas de publications inappropriées.

c. Surveillance NSS

La fonctionnalité SSN Watch vous avertit lorsque de nouveaux noms ou adresses sont associés à votre numéro de sécurité sociale.

2. Assurance et récupération

Lookout vous aide à surmonter l'épreuve de récupérer votre identité en cas de vol.

a. Assurance contre le vol d'identité

Lookout Premium Plus couvre vos frais juridiques, les salaires perdus et autres frais liés à la récupération de votre identité volée.

b. Assistance à la récupération

Les spécialistes de la récupération d'identité de Lookout sont à vos côtés 7 jours sur 7 et 24 heures sur 24 pour vous aider à récupérer votre identité en cas de vol.

c. Récupération de portefeuille perdu

Lookout vous aide à faire opposition et à remplacer les cartes bancaires, pièces d'identité et autres documents de votre portefeuille en cas de vol ou de perte.

8. Service client d'opérateur mobile pour les clients KDDI

Si votre opérateur mobile participe à notre programme Mobile Operator Customer Care, vous pouvez l'appeler pour retrouver et sécuriser votre téléphone ou votre tablette en cas de perte ou de vol.

Afin de permettre à Lookout de délivrer des services client, nous avons besoin de certaines informations à votre sujet et celui de votre appareil. L'application Customer Care Web recueille votre numéro de téléphone (si disponible), ainsi que des informations sur le type d'appareil et système d'exploitation que vous utilisez,

pour permettre aux représentants du service client d'identifier avec exactitude et de gérer à distance les fonctions de votre appareil.

Lookout se sert de vos informations pour informer le représentant du service client qu'il peut fournir le niveau de service client prévu.

L'application Customer Care Web permet aux opérateurs mobiles et aux représentants de leur service client d'exécuter des fonctions à distance sur votre appareil à votre demande, notamment :

- Localiser l'appareil ;
- Verrouiller l'appareil ;
- Effacer les données de l'appareil ;
- Activer une sirène stridente (Scream) ;
- Envoyer un message à l'appareil.

Les représentants du service client peuvent exécuter ces fonctions uniquement à votre demande et avec votre consentement préalable.

Le cas échéant, Lookout vous prévient en vous envoyant un e-mail à l'adresse électronique enregistrée pour protéger votre vie privée. Les représentants du service client ne contrôlent pas les données des utilisateurs sauvegardées à l'aide de l'application mobile de Lookout et n'y ont pas accès.

9. Analyse des données - Comment nous utilisons les informations recueillies à partir de votre appareil de point de terminaison mobile

Nous sommes susceptibles d'utiliser les résultats de nos analyses de données pour vous envoyer du contenu pertinent, vous proposer de nouvelles fonctionnalités, de nouveaux produits et/ou services afin d'améliorer votre expérience des services Lookout. Nous n'associons pas les informations que nous stockons dans le logiciel d'analyse aux données à caractère personnel que vous nous communiquez via l'application mobile. Par ailleurs, les informations sous forme agrégée sont rendues anonymes pour empêcher l'identification d'un individu.

En plus d'utiliser les informations que vous nous communiquez et celles que nous recueillons à partir de votre point de terminaison mobile pour vous délivrer les services Lookout, nous utilisons les informations recueillies à partir de votre appareil à des fins d'analyse de données. Ces analyses nous fournissent des informations très utiles qui nous permettent d'améliorer les fonctionnalités et l'ergonomie de nos produits. Parmi les informations que nous analysons figurent la fréquence d'utilisation de l'application Lookout sur votre appareil,

les événements internes qui surviennent au sein de l'application sur votre appareil et le site depuis lequel vous avez téléchargé l'application Lookout sur votre appareil mobile. Nous utilisons également ces informations sous forme agrégée pour analyser les menaces mobiles connues et nouvelles.

10. Votre utilisation du site Web de Lookout et du site Web mobile et les informations recueillies

Lorsque vous utilisez le site Web Lookout sur votre ordinateur ou sur votre point de terminaison mobile, Lookout est susceptible de recueillir de sa propre initiative des informations à votre sujet pour améliorer votre expérience utilisateur. Lookout peut aussi avoir recours à des services d'analyse pour mesurer la façon dont notre site Web et nos e-mails sont utilisés, ce qui nous aide à améliorer nos produits et services et à vous proposer des contenus plus pertinents. Pour fonctionner, ces services d'analyse peuvent intégrer des images invisibles associées à un identifiant unique à notre site Web ou site Web mobile, déposer des cookies ou d'autres dispositifs de stockage local sur l'appareil ou utiliser des balises Web, des pixels espions, des images gif transparentes et des technologies de suivi similaires.

a. Contenu et promotions

Nous pouvons vous demander d'indiquer votre adresse électronique et vos autres coordonnées lors de votre visite de nos sites Web pour accéder à divers contenus Lookout, tels que des livres blancs, des vidéos ou d'autres documents de recherche. Nous sommes également susceptibles de vous demander de participer à des enquêtes, des concours, des promotions ou des tirages au sort. Nous pouvons vous demander votre avis concernant votre expérience avec les produits et services Lookout. Vos coordonnées nous servent à vous fournir de plus amples informations sur les produits et services de Lookout ou de ses partenaires commerciaux. Vous pouvez refuser de recevoir ces communications marketing en cliquant sur le lien de désabonnement de nos e-mails, comme expliqué ci-dessous.

b. Fonctionnalités de réseaux sociaux

Notre site Web intègre des fonctionnalités de réseaux sociaux (les « Fonctionnalités ») telles que le bouton « J'aime » sur Facebook ou des mini-programmes interactifs exécutés sur notre site. Si vous les utilisez, ces fonctionnalités recueilleront votre adresse IP et la page que vous consultez sur notre site. Elles déposeront également un cookie afin de fonctionner correctement. Ces Fonctionnalités peuvent être hébergées par un tiers ou directement sur notre site. Vos interactions avec ces Fonctionnalités tiers sont régies par la politique de confidentialité de la société qui fournit ladite Fonctionnalité et non par la Politique de confidentialité de Lookout.

11. Politique relative aux cookies du site Web de Lookout

1. Types de cookies

Comme de nombreux services en ligne, nous utilisons des cookies et d'autres outils pour recueillir et analyser des informations à votre sujet et sur votre utilisation de nos produits et services. Nous utilisons ces technologies afin de proposer du contenu pertinent concernant les produits et services Lookout. Les cookies sont de petits fichiers de données que nous stockons sur votre ordinateur ou votre appareil. Pour en savoir plus, rendez-vous sur aboutcookies.org.

2. Utilisation des cookies

Nous utilisons des « cookies de session » pour maintenir votre connexion pendant que vous utilisez nos services, pour mieux comprendre vos interactions avec ces derniers et pour surveiller des informations agrégées sur l'utilisation de ces services et le trafic Web associé. Les cookies de session disparaissent dès que vous vous déconnectez et fermez le navigateur. Nous utilisons également des « cookies persistants » pour vous reconnaître lorsque vous faites à nouvel appel à nos services. Les cookies persistants peuvent rester plus longtemps sur votre ordinateur que les cookies de session. Nous utilisons par ailleurs des « cookies d'analyse ». Ils nous permettent de reconnaître les utilisateurs, de les compter et de savoir comment ils parcourent et utilisent nos services. Ces informations nous permettent d'améliorer le fonctionnement de notre site Web, par exemple en nous assurant que les utilisateurs trouvent facilement ce qu'ils cherchent. Enfin, nous pouvons avoir recours à d'autres technologies standard, telles que des balises Web, des pixels espions, des images gif transparentes et des dispositifs de stockage local, afin d'analyser, de recueillir et d'agréger les données d'utilisation de nos produits et services.

3. Cookies tiers

Nous estimons qu'il est important que vous sachiez exactement quels cookies tiers nous utilisons sur notre site Web et dans le cadre de nos services. Voici une liste des cookies tiers que nous utilisons et qui peuvent recueillir des Données à caractère personnel sur vos activités en ligne au fil du temps et sur des services en ligne ou des sites Web tiers. À mesure que nous développons et améliorons nos services, nous pouvons être amenés à en utiliser d'autres et à mettre à jour cette liste en conséquence. Nous avons également inclus un lien vers la politique de confidentialité qui régit les cookies tiers.

- Google Analytics : ces cookies nous permettent de savoir comment vous utilisez notre site Web et notre application mobile afin d'améliorer votre expérience. Nous vous encourageons à consulter les [Règles de confidentialité de Google](#). Si vous ne souhaitez pas que Google Analytics utilise vos données dans ses rapports, Google vous permet de vous y opposer en installant le [module complémentaire de navigateur pour la désactivation de Google Analytics](#).

- Google AdWords : ces cookies permettent à nos fournisseurs de diffuser des annonces en fonction de vos précédentes visites sur nos sites et de mener des activités de remarketing. Google peut utiliser ce type de cookies, ainsi que d'autres technologies de suivi, pour vous présenter nos annonces sur d'autres sites Web. Google vous permet de refuser l'utilisation de ces cookies en accédant aux [Paramètres des annonces](#) de Google.
- Marketo : ces cookies nous aident à suivre vos visites sur notre site Web et à vous offrir une expérience marketing agréable. Nous les utilisons également pour comprendre vos interactions avec les e-mails que nous vous envoyons et pour nous assurer que nous vous communiquons des informations pertinentes. Par exemple, les cookies Marketo nous permettent de savoir si vous lisez nos e-mails et sur quels liens vous cliquez. Vous pouvez consulter la [Politique de confidentialité de Marketo ici](#).
- Fonctionnalités de réseaux sociaux : notre site Web intègre des fonctionnalités de réseaux sociaux, comme des boutons de recommandation ou des mini-programmes exécutés sur notre site. Lorsque vous les utilisez, ces Fonctionnalités recueillent votre adresse IP et la page que vous consultez sur notre site. Elles déposent également un cookie afin de fonctionner correctement. Ces Fonctionnalités peuvent être hébergées par un tiers ou directement sur notre site. Vos interactions avec ces fonctionnalités sont régies par la politique de confidentialité de la société qui les fournit et non par la Politique de confidentialité de Lookout.
- Mixpanel, Braze et mParticle : ces cookies nous permettent d'analyser et d'agréger les données d'utilisation de notre application mobile. Nous vous encourageons à consulter la [Politique de confidentialité de MixPanel](#), la [Politique de confidentialité de Braze](#) et la [Politique de confidentialité de mParticle](#).

12. Base légale de l'utilisation de vos informations

La base légale de l'utilisation de vos informations, telle que définie dans la présente Politique de confidentialité, est la suivante : (a) l'utilisation de vos Données à caractère personnel est nécessaire pour nous acquitter de nos obligations en vertu de tout contrat conclu avec vous (par exemple, pour respecter les Conditions d'utilisation que vous avez acceptées en téléchargeant et en utilisant nos applications) ; ou (b) si l'utilisation de vos informations n'est pas nécessaire à l'exécution d'un contrat, elle l'est néanmoins pour nos intérêts légitimes ou ceux d'autrui (par exemple, pour garantir la sécurité des services Lookout, exploiter et commercialiser les services Lookout, assurer la sécurité des environnements pour notre personnel et les autres, effectuer et percevoir des paiements, empêcher la fraude et connaître le client à qui nous fournissons les services Lookout). Une partie du traitement est requise par la législation en vigueur.

Dans certains cas (dans le cadre de certaines activités marketing par exemple), nous pouvons traiter vos Données à caractère personnel après avoir reçu votre consentement.

Outre les utilisations spécifiques décrites ci-dessus, nous utilisons vos informations des manières suivantes :

a. Nous utilisons vos informations pour fournir, améliorer et promouvoir nos services

Nous utilisons vos informations pour mieux vous servir, pour améliorer nos produits et services, pour les promouvoir et pour en développer de nouveaux. Par exemple :

- Si vous répondez à une enquête ou envoyez un e-mail à Lookout pour obtenir de l'aide, nous pouvons conserver ces informations afin de vous fournir une assistance et d'améliorer nos services.
- Lorsqu'elles sont disponibles, Lookout peut utiliser les informations de l'appareil client pour vous avertir que vous devez mettre à jour le système d'exploitation.
- Nous pouvons envoyer des SMS à votre téléphone pour communiquer avec celui-ci.
- Nous pouvons utiliser votre adresse électronique ou votre numéro de téléphone mobile pour vous envoyer des notifications liées à la confidentialité ou à la sécurité et vous avertir de toute modification importante des services Lookout.
- Nous pouvons utiliser votre adresse électronique ou votre numéro de téléphone mobile pour vous informer des annonces de produits et des offres spéciales de Lookout ou de ses partenaires commerciaux, ou pour gérer la participation à des événements spéciaux, enquêtes, concours et tirages au sort.
- Nous pouvons utiliser vos informations pour réaliser des études de marché et participer à des activités promotionnelles conjointes avec des sociétés proposant des produits qui peuvent apporter une valeur ajoutée aux produits ou services Lookout (par ex. : avec des opérateurs mobiles).

b. Nous pouvons divulguer vos informations conformément à la législation

Comme d'autres sociétés, nous pouvons divulguer vos informations conformément à la législation, par exemple pour : (i) respecter une loi, une réglementation ou une procédure judiciaire (y compris pour respecter des exigences de sécurité nationale ou des forces de l'ordre) ; (ii) préserver la sécurité de toute personne, entité ou installation ; (iii) traiter les violations potentielles de notre Politique de confidentialité ou de nos Conditions d'utilisation ; (iv) enquêter sur tout problème de fraude, de sécurité ou technique ; ou (v) protéger les droits ou les biens de Lookout ou d'un tiers, nos employés, les utilisateurs et le public.

Nous sommes convaincus que vous êtes en droit de savoir si nous sommes légalement tenus de divulguer vos

informations. Par conséquent, avant de divulguer vos informations à la suite d'une demande des autorités (par exemple, une assignation ou une ordonnance de tribunal), nous vous préviendrons à l'adresse électronique associée à votre compte, sauf si (a) cela nous est interdit ou (b) il s'agit d'une urgence et vous prévenir pourrait entraîner un risque de blessure ou de décès, ou l'affaire implique une atteinte potentielle à un mineur. Par ailleurs, rien dans la présente Politique de confidentialité ne saurait limiter les défenses ou objections que vous êtes légalement en droit d'opposer à une demande de divulgation de vos informations émanant d'un tiers, y compris d'un gouvernement.

c. Nous partageons vos informations afin de fournir ou d'améliorer nos services

Nous partageons vos informations avec d'autres membres de notre groupe ou avec des tierces parties afin de fournir ou d'améliorer nos services. Par exemple :

- Nous pouvons partager vos informations avec des fournisseurs de services et produits tiers intégrés à nos logiciels qui ont besoin de connaître ces informations pour répondre à vos demandes (par exemple, pour vous localiser sur une carte, vous envoyer un SMS ou vous fournir des services de protection d'identité), pour prendre en charge nos produits et services ou pour analyser les données afin d'améliorer les produits et leurs performances.
- Nous sommes susceptibles de partager vos informations avec des opérateurs mobiles qui participent à notre programme Mobile Operator Customer Care afin qu'ils puissent vous aider directement à utiliser les fonctionnalités Missing Device de Lookout, telles que la localisation à distance, le verrouillage, l'effacement des données ou Scream via notre application Web Customer Care, sur demande de votre part.
- Nous pouvons partager vos informations dans le cadre de nos activités de comptabilité, d'audit, de rapprochement des factures et de recouvrement.
- Nous sommes susceptibles de partager vos informations avec nos sociétés affiliées, revendeurs ou autres fournisseurs de services tiers qui collaborent avec Lookout (par exemple, des opérateurs mobiles et des fournisseurs MDM) pour assurer la bonne livraison de votre achat et les services d'assistance associés, accomplir certaines fonctions professionnelles et vous fournir des informations concernant les produits et services.

13. Vos données peuvent être incluses à des rapports de sécurité

En vue de réaliser des analyses de données, nous rendons anonymes, agrégeons et résumons les données, qui peuvent contenir certaines des vôtres. Nous sommes susceptibles de divulguer vos informations avec votre

accord. Nous sommes également susceptibles de partager vos Données à caractère personnel avec des tiers dès lors que vous nous y autorisez.

14. Vos choix

a. Vous pouvez accéder à vos paramètres et les mettre à jour

Votre compte Lookout sur notre site Web et/ou la page « Paramètres » de notre application mobile vous permettent de mettre à jour ou de modifier certains paramètres qui influent sur les données qui nous sont communiquées (par ex. : en désactivant la sauvegarde de certains types de données). Dans le souci de préserver votre sécurité et votre vie privée, nous vous demandons votre nom d'utilisateur et votre mot de passe afin de vérifier votre identité avant de vous permettre d'accéder à votre compte ou d'effectuer des modifications. Si vous souhaitez corriger ou supprimer des Données à caractère personnel inexactes ou accéder à toute donnée à caractère personnel que nous détenons à votre sujet, veuillez nous contacter à l'adresse privacy@lookout.com. Nous nous engageons à répondre à votre demande d'accès dans les 30 jours. Cependant, dans certaines situations, Lookout n'est pas en mesure de vous donner accès à toutes les Données à caractère personnel détenues à votre sujet ou de les supprimer.

b. Désabonnement aux e-mails

Vous pouvez refuser de recevoir des communications promotionnelles de la part de Lookout en utilisant le lien de désabonnement présent dans chaque e-mail. Bien que les demandes de désabonnement soient généralement traitées immédiatement, veuillez prévoir un délai de dix (10) jours ouvrés avant qu'elles deviennent effectives. Même si vous refusez de recevoir des messages promotionnels de notre part, vous continuerez à recevoir des messages relatifs à vos transactions et à vos produits dans le cadre des Services Lookout. Vous pouvez refuser certains de ces messages de notification dans les paramètres de votre compte.

c. Publicités personnalisées

Vous pouvez refuser de recevoir certaines publicités personnalisées de la part de sociétés qui sont membres de la Network Advertising Initiative ou qui souscrivent aux Principes d'autorégulation de la publicité comportementale en ligne de la Digital Advertising Alliance. Veuillez consulter la [page de désabonnement des consommateurs de la Network Advertising Initiative](#) ou la [page de désabonnement de la Digital Advertising Alliance](#) pour vous désabonner directement auprès des fournisseurs qui participent à ces programmes. Lookout ne contrôle pas et ne gère pas ces outils ni les choix proposés par les annonceurs et autres sociétés par le biais de ces outils.

d. Localisation

Lorsque vous supprimez les données de localisation via le tableau de bord de votre compte sur Lookout.com, ces données ne sont plus liées à votre compte et sont rendues anonymes dans nos systèmes de production d'application.

15. Politique de conservation des données

Notre politique consiste à ne conserver les Données à caractère personnel que pendant la durée raisonnablement nécessaire pour vous fournir nos produits et services ou pour respecter les exigences légales. Nous sommes susceptibles de supprimer vos données si votre compte est inactif et dans les autres cas prévus dans nos Conditions d'utilisation.

16. Les informations publiées sur notre blog et notre forum communautaire sont publiques

Si vous saisissez des commentaires sur notre blog ou nos autres forums publics, vous devez garder à l'esprit que les autres utilisateurs peuvent les lire, les recueillir ou les utiliser, y compris pour vous envoyer des messages indésirables. Nous ne sommes pas responsables des informations que vous choisissez de partager sur ces blogs ni du contenu que vous recevez en conséquence de ce partage.

17. Nous prenons la sécurité au sérieux

Lookout est une société spécialisée dans la sécurité. Nous accordons donc une grande importance à la sécurité de vos données. Lookout utilise des techniques de protection physiques, organisationnelles et techniques commercialement raisonnables pour mettre en œuvre des mesures techniques et organisationnelles appropriées. Par exemple, nous combinons divers dispositifs de pare-feu, d'authentification, de sécurité physique et autres pour protéger votre compte et vos données. Lorsque vous saisissez des informations sensibles (telles que votre numéro de carte de crédit ou des informations de localisation) sur notre site Web, dans l'application Lookout ou sur nos formulaires de commande, nous les transmettons sous forme chiffrée à l'aide de la technologie SSL (Secure Sockets Layer). Nous confions également la réalisation de tests d'intrusion à des tierces parties afin de renforcer nos systèmes contre les attaques. Lookout déploie tous les efforts raisonnables pour mettre en place des contrôles afin de se protéger contre les menaces technologiques complexes et autres menaces criminelles et se prémunir face aux employés négligents.

Aucune méthode de transmission via Internet ou de stockage électronique n'étant sûre à 100 %, nous ne pouvons pas assurer ni garantir la sécurité des informations, données ou contenus que vous nous transmettez

ou que nous recevons pour votre compte afin de gérer les services Lookout. La réception et la transmission de vos informations s'effectuent de votre plein gré et à vos risques et périls. Nous ne saurions garantir que ces informations ne feront l'objet d'aucun accès et d'aucune divulgation, modification ou destruction résultant d'une faille de nos mesures de protection physiques, organisationnelles ou techniques.

Si Lookout prend connaissance d'une faille de sécurité, nous nous engageons à tenter de vous avertir par voie électronique afin que vous preniez les mesures de protection appropriées. Lookout s'engage également à publier une notification sur les services Lookout dans un tel cas. En fonction de votre pays de résidence, vous pouvez être légalement en droit de recevoir une notification écrite en cas de faille de sécurité.

18. Vous êtes responsable de l'exactitude et de la confidentialité de votre adresse électronique et de votre mot de passe

Il vous incombe de veiller en permanence à la confidentialité de votre mot de passe. Nous vous recommandons de choisir un mot de passe fort que vous n'utiliserez avec aucun autre service. Si vous pensez que votre mot de passe a été compromis, changez-en immédiatement sur le site Web de Lookout ou contactez-nous à l'adresse support@lookout.com pour obtenir de l'aide. Il vous incombe de veiller à ce que l'adresse électronique associée à votre compte soit exacte. Nous utilisons cette adresse pour vous contacter au sujet des mises à jour des services, des modifications de nos politiques et des activités de votre compte telles que les demandes d'accès à vos informations ou les tentatives de localisation sur votre appareil. Lookout n'est pas responsable des Données à caractère personnel transmises à un tiers en raison d'une adresse électronique incorrecte fournie par l'utilisateur.

19. Avis aux utilisateurs californiens

a. Do Not Track

Do Not Track est une préférence de confidentialité que les utilisateurs peuvent définir sur leur navigateur Web. Lorsque le signal Do Not Track est activé, le navigateur envoie aux sites Web un message leur demandant de ne pas suivre l'utilisateur. Pour en savoir plus sur Do Not Track, rendez-vous sur www.allaboutdnt.org. À l'heure actuelle, nous ne prenons pas en compte les paramètres de navigateur ou signaux Do Not Track. Par ailleurs, certains de nos fournisseurs de services tiers peuvent utiliser des technologies standard, telles que des cookies, des pixels invisibles et des balises Web pour recueillir des informations à propos de vos activités sur Internet. Vous pouvez désactiver le suivi entre sites mis en place par certaines tierces parties en vous reportant à l'article « Vos choix » ci-dessus.

20. Visiteurs internationaux, Privacy Shield et RGPD

Lookout est une société basée à San Francisco et ses serveurs sont hébergés aux États-Unis. Les Données à caractère personnel recueillies auprès d'utilisateurs d'autres pays sont transférées aux États-Unis. Si vous utilisez les services Lookout depuis un autre pays, vos informations sont susceptibles d'être transférées, stockées et traitées aux États-Unis, où se trouvent nos serveurs et où sont gérées nos bases de données. Lookout a suivi le processus de certification [Privacy Shield](#) mis en place par le ministère du Commerce des États-Unis concernant le recueil, l'utilisation et la conservation des données à caractère personnel qui proviennent des états membres de l'UE et de Suisse. Les principes du Privacy Shield définissent un cadre d'exigences régissant l'utilisation et le traitement par les sociétés participantes des Données à caractère personnel recueillies au sein de l'UE et de la Suisse. En adhérant au Privacy Shield, les participants s'engagent à respecter ces principes qui s'appliquent en vertu de la législation américaine. Lookout certifie qu'elle respecte les principes du Privacy Shield en matière de notification, de choix, de transfert ultérieur, de sécurité, d'intégrité des données, d'accès et d'application pour ces Données à caractère personnel. Pour en savoir plus sur le Privacy Shield et consulter la liste des entités actuellement certifiées ou la certification de Lookout, rendez-vous sur <http://www.privacyshield.gov>.

Conformément à ces principes, lorsque Lookout reçoit des informations concernées par le Privacy Shield, puis les transfère à un fournisseur de services tiers agissant pour son compte en tant qu'agent, elle est responsable dans une certaine mesure en vertu du Privacy Shield si : (i) l'agent traite les informations d'une façon contraire au Privacy Shield et (ii) Lookout est responsable de l'événement à l'origine du préjudice.

Pour toute question ou réclamation concernant les pratiques de Lookout en matière de confidentialité, y compris dans le cadre du Privacy Shield, vous pouvez nous contacter à privacy@lookout.com ou à l'adresse postale indiquée à l'article « Contactez-nous pour toute question ou préoccupation ». Nous collaborerons avec vous pour résoudre le problème.

Si vous résidez au sein de l'Union européenne et que vous n'êtes pas satisfait(e) de la façon dont nous avons traité votre problème concernant nos pratiques de confidentialité, vous pouvez demander une assistance supplémentaire gratuite par le biais de notre mécanisme de recours indépendant dédié au Privacy Shield. Pour en savoir plus, rendez-vous sur <https://www.jamsadr.com/eu-us-privacy-shield>. Vous avez également le droit de déposer plainte auprès de l'autorité de contrôle compétente. Nous vous invitons, cependant, à nous contacter en premier et nous nous efforcerons de résoudre votre problème.

Les résidents de l'Union européenne peuvent aussi recourir à l'arbitrage des réclamations non résolues, mais auparavant, ils doivent : (1) contacter Lookout pour lui donner une chance de résoudre le problème ; (2) demander l'assistance du mécanisme de recours indépendant dédié de Lookout mentionné ci-dessus ; et

(3) contacter le ministère du Commerce des États-Unis (directement ou par l'intermédiaire d'une autorité européenne chargée de la protection des données) et lui laisser le temps de tenter de résoudre le problème. Chacune des parties devra s'acquitter de ses propres honoraires d'avocat. Veuillez noter qu'en vertu du Privacy Shield, le ou les arbitres peuvent uniquement imposer des mesures de redressement non pécuniaires et propres à la personne concernée afin de remédier à une violation des principes du Privacy Shield à l'égard de cette personne. Lookout est soumise aux pouvoirs d'enquête et d'exécution de l'U.S. Federal Trade Commission (FTC).

Outre les droits accordés en vertu de l'article ci-dessus intitulé « Vous pouvez accéder à vos paramètres et les mettre à jour », certains utilisateurs internationaux (y compris ceux dont nous recueillons les informations dans le cadre du Privacy Shield) disposent légalement d'un droit d'accès et de suppression de certaines informations que nous détenons à leur sujet. Pour exercer ce droit, ils peuvent nous contacter à l'adresse privacy@lookout.com en indiquant leur demande.

L'Union européenne a pris une mesure pour protéger le droit fondamental à la vie privée pour les résidents européens avec le Règlement général pour la protection des données (RGPD) qui entrera en vigueur le 25 mai 2018. Toute société qui traite des Données à caractère personnel de résidents européens de quelque manière que ce soit est tenue de protéger ces données. Lookout déploie tous les efforts raisonnables et prend les mesures techniques et organisationnelles préconisées pour respecter le Règlement général pour la protection des données (Règlement (UE) 2016/679) (« RGPD »).

Ces efforts comprennent :

Déterminer le type de Données à caractère personnel - Chaque service Lookout requiert un niveau différent de recueil, d'utilisation, de stockage et de suppression des Données à caractère personnel. En définissant la portée des Données à caractère personnel de chacun de ces services et en documentant les différentes sources de données, nous pouvons déterminer le type de Données à caractère personnel que nous recevons afin de permettre à Lookout de gérer et de protéger ces actifs essentiels comme il se doit.

Assurer la visibilité et la transparence - Lookout assure la transparence de son traitement et l'accès aux Données à caractère personnel en répondant aux demandes des clients dans les plus brefs délais conformément aux exigences du RGPD. Pour envoyer une demande, veuillez contacter support@lookout.com. Vous pouvez consulter et mettre à jour vos Données à caractère personnel en accédant à votre portail en ligne Lookout personnalisé.

Garantir la sécurité et l'intégrité des données - Afin de préserver l'intégrité des données, Lookout gère les accès aux données des clients en appliquant des contrôles d'accès très stricts. Lookout met également en

œuvre des mesures de sécurité appropriées en chiffrant les Données à caractère personnel lors de leur stockage et de leur transmission.

21. Utilisateurs de moins de 16 ans

Lookout offre ses services à une clientèle internationale. En vue de respecter les exigences légales américaines et européennes associées au Chapitre 91 du Children's Online Privacy Protection Act et à l'Article 8 Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information du RGPD, Lookout atteste ne pas recueillir ni stocker sciemment des Données à caractère personnel concernant des enfants de moins de 16 ans, hormis dans le cadre d'un Forfait pour plusieurs appareils achetés par un parent qui accepte le recueil et le stockage des données, tels que décrits dans les Conditions d'utilisation de Lookout. Si vous pensez qu'un enfant utilise ce service sans accord parental, veuillez nous contacter à l'adresse privacy@lookout.com.

22. Nous ne sommes pas responsables du contenu des sites Web tiers

Notre site contient des liens vers d'autres sites Web. Lorsque vous cliquez sur l'un de ces liens, vous quittez le site Web de Lookout pour accéder à un autre site. Lookout décline toute responsabilité en cas d'utilisation abusive de toute information par le responsable d'un site Web vers lequel nous proposons un lien. Nous vous encourageons à consulter les déclarations de confidentialité de ces sites liés, car elles peuvent être différentes de la nôtre. Par ailleurs, si vous profitez d'une offre de l'un de nos partenaires, vous fournirez peut-être des informations directement à ce dernier. Nous vous encourageons à consulter les déclarations de confidentialité de ces partenaires, car nous ne sommes pas responsables de leurs pratiques en la matière ni de celles des sites liés.

23. Changement de contrôle

En cas de faillite, de fusion, d'acquisition, de restructuration ou de vente d'actifs impliquant Lookout, vos informations sont susceptibles d'être vendues ou cédées dans le cadre de la transaction en question.

24. Toute modification de cette politique fait l'objet d'un avis sur notre site Web

Nous sommes susceptibles de réviser la présente Politique de confidentialité suivant l'évolution de nos produits et services et des lois applicables à Lookout et à vous-même. En cas de modification substantielle de la présente politique, nous vous préviendrons par le biais de notre application, sur ce site Web, par e-mail ou en publiant un avis sur la page d'accueil de Lookout. En continuant d'utiliser nos services, vous indiquez que vous acceptez la nouvelle Politique de confidentialité et que vous consentez à être lié(e) par celle-ci. Si vous

refusez que vos informations soient soumises à la Politique de confidentialité révisée, vous devez résilier votre compte.

25. Contactez-nous pour toute question ou préoccupation

Veillez contacter notre Responsable de la protection des données à privacy@lookout.com ou par courrier à Lookout, Inc., Attn : Michael Musi, Data Privacy Officer, One Front Street, Suite 3100 San Francisco, CA 94111, États-Unis, pour nous faire part de toute question ou de tout commentaire en relation avec la présente politique. Les résidents de l'UE peuvent également envoyer leurs demandes à l'attention de M. G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Pays-Bas.