
Lookout, Inc.
Application Personal
Déclaration de confidentialité

Date d'entrée en vigueur :
01/01/2020
Date de création :
15/11/2016
Date de révision : 01/01/2020

1. INTRODUCTION	3
2. INFORMATIONS COLLECTÉES PAR LOOKOUT.	3
A. CATEGORIES D'INFORMATIONS. LOOKOUT, OU LES PARTENAIRES DE LOOKOUT, PEUVENT COLLECTER LES CATEGORIES D'INFORMATIONS SUIVANTES AUPRES DE VOUS LORSQUE VOUS UTILISEZ L'APPLICATION PERSONAL :	3
B. INFORMATIONS COLLECTÉES PAR LOOKOUT POUR L'APPLICATION LOOKOUT BASIC PERSONAL	4
C. INFORMATIONS COLLECTÉES PAR LOOKOUT POUR L'APPLICATION LOOKOUT PREMIUM PERSONAL	4
D. INFORMATIONS COLLECTÉES PAR LOOKOUT POUR L'APPLICATION LOOKOUT PREMIUM PLUS PERSONAL	5
E. INFORMATIONS COLLECTÉES PAR LOOKOUT AUPRES DE TIERS.	5
LOOKOUT REÇOIT DES DONNÉES D'ANALYSE TRANSMISES PAR DES TIERS, COMME DECRIT CI-DESSUS.	5
3. UTILISATION DE VOS INFORMATIONS.	5
4. DIVULGATION DES INFORMATIONS	6
5. VOS CHOIX	7
A. VOUS POUVEZ ACCÉDER A VOS PARAMÈTRES ET LES METTRE A JOUR	8
B. DESABONNEMENT AUX E-MAILS	8
6. CONSERVATION DES DONNÉES	8
7. SÉCURITÉ	8
A. RESPONSABILITÉS DE LOOKOUT.	8
B. VOS RESPONSABILITÉS	8
8. UTILISATEURS DE MOINS DE 16 ANS	9
9. TRANSFERTS DE DONNÉES INTERNATIONAUX	9
10. CONDITIONS SUPPLÉMENTAIRES POUR LES RÉSIDENTS DE L'ESPACE ÉCONOMIQUE EUROPÉEN (EEE)	9
A. BASE LÉGALE DE TRAITEMENT.	9
B. VOS DROITS.	10
11. CONTACTEZ-NOUS POUR TOUTE QUESTION OU PRÉOCCUPATION	11

1. Introduction

Le présent document constitue notre Déclaration de confidentialité pour l'Application Personal (la « Déclaration »). Il décrit les informations que nous collectons auprès de vous lorsque vous utilisez l'Application Lookout Personal (l'« Application Personal ») et la manière dont nous utilisons ces informations. Nous vous recommandons de lire la Déclaration, ainsi que les [Conditions d'utilisation](#) de Lookout (disponibles à l'adresse www.lookout.com/legal/terms), car les deux documents concernent votre utilisation de l'Application Personal. Toutes les informations collectées auprès de vous par Lookout autrement que dans le cadre de l'utilisation de l'Application Personal seront soumises à une déclaration de confidentialité distincte.

Nous pouvons modifier la présente Déclaration suivant l'évolution de nos produits et services et des lois applicables à Lookout et à vous-même. Nous vous informerons de toute modification substantielle apportée à la présente Déclaration. Si vous refusez que vos informations soient soumises à la Déclaration modifiée, vous devrez résilier votre compte.

Vous pouvez accéder à la présente Déclaration à partir de l'écran de connexion de l'application mobile Lookout ou des paramètres de l'Application Lookout Personal, ainsi que sur le site Web de notre société.

2. Informations collectées par Lookout.

Lookout propose différents niveaux au sein de l'Application 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 collectons directement auprès de vous, à partir de votre appareil et comment nous utilisons ces informations. Pour en savoir plus sur les fonctionnalités de l'Application Personal pour les appareils iOS et Android, consultez les pages <https://www.lookout.com/products/personal/ios> et <https://www.lookout.com/products/personal/android>.

- a. **Catégories d'informations.** Lookout, ou les partenaires de Lookout, peuvent collecter les catégories d'informations suivantes auprès de vous lorsque vous utilisez l'Application Personal :
 - i. **Données d'inscription**, y compris adresse e-mail et mot de passe.
 - ii. **Données de l'appareil**, telles que l'identifiant du matériel (p. ex., numéro de téléphone, type et fabricant de l'appareil, type et version du système d'exploitation, opérateur, type de réseau, pays d'origine, SSID du réseau Wi-Fi, adresse IP, dates et heures de vos requêtes).
 - iii. **Données d'applications**, y compris les métadonnées de toutes les applications installées sur votre appareil mobile (y compris, sans toutefois s'y limiter, les noms et versions des applications). Dans certains cas, nous pouvons également collecter une copie totale ou partielle de fichiers d'applications présents sur votre appareil si nous détectons une application que nous n'avons pas encore analysée. Ces données sont rendues anonymes et sont conservées sous forme agrégée afin d'empêcher toute identification d'un individu par d'autres clients. Nous pouvons également collecter des informations relatives au comportement des applications sur votre appareil (p. 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.
 - iv. **Données 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 collecter des informations de localisation de deux manières : soit directement sur votre appareil mobile, soit (dans certains cas) grâce aux données de localisation envoyées par une antenne relais ou un point d'accès Wi-Fi. Nous pouvons faire appel à des fournisseurs de services tiers pour convertir ces données en informations de localisation exploitables. Si vous souhaitez empêcher tout partage des données de localisation, accédez aux paramètres de votre appareil mobile et désactivez les services de localisation. Notez toutefois que cela peut avoir un impact sur les fonctionnalités proposées par Lookout.
 - v. **Données sur les alertes de vol**, y compris des Données de localisation et une photo capturée lorsque la fonctionnalité Theft Alerts s'active.

- vi. **Données de paiement**, y compris le numéro, la date d'expiration et le code de sécurité de votre carte bancaire ainsi que d'autres informations de facturation applicables, qui peuvent être collectées directement par nos partenaires si vous avez acheté les versions Premium ou Premium Plus de l'application.
- vii. **Données de contenu Web**, y compris les URL et les noms de domaines associés à des contenus malveillants ou nécessitant une analyse supplémentaire afin de déterminer s'ils sont dangereux (p. ex., si les URL contiennent des attaques par phishing ou des logiciels malveillants). Lookout ne collecte pas votre historique de navigation.
- viii. **Données de protection contre le vol d'identité**, que vous pouvez fournir si vous avez acheté un abonnement Lookout Premium Plus, y compris des informations personnelles (p. ex., numéro de permis de conduire, de sécurité sociale, de passeport, ou autre numéro d'identification), des informations financières (p. ex., numéros de compte bancaire et de carte de crédit/débit), votre numéro d'assurance maladie et d'autres informations personnelles (p. ex., nom et titre) vous concernant (vous-même ou d'autres personnes que vous inscrivez à ce service). Ces données peuvent être collectées directement par notre partenaire CSIdentity (désormais affilié à Experian).
- ix. **Données d'analyse**, y compris des données d'outils tiers tels que Mixpanel, Braze et mParticle. Ces données nous permettent d'analyser et d'agréger les données concernant votre utilisation de nos Services. Nous vous encourageons à consulter la [Politique de confidentialité de Mixpanel](#), la [Politique de confidentialité de Braze](#) et la [Politique de confidentialité de mParticle](#).

Les fonctionnalités disponibles varient selon le niveau choisi. Aussi, Lookout peut collecter différents types d'informations selon le niveau que vous utilisez, comme décrit ci-dessous.

b. Informations collectées par Lookout pour l'Application Lookout Basic Personal

- i. **Données d'inscription**. Afin de créer un compte, vous devez indiquer votre adresse e-mail, ainsi qu'un mot de passe.
- ii. **Données de l'appareil**. Lorsque vous utilisez les Services Lookout, nos serveurs enregistrent certaines informations relatives à votre appareil mobile, comme décrit dans la Section 2(a)(ii) ci-dessus.
- iii. **Données d'applications**. Lorsque vous utilisez les Services Lookout, nous collectons des fichiers d'applications et nous téléchargeons une copie totale ou partielle de fichiers d'applications présents sur votre appareil si nous détectons une application que nous n'avons pas encore analysée, comme décrit dans la Section 2(a)(iii) ci-dessus. Nous ne collectons pas les données utilisateur que vous saisissez dans ces applications. Nous ne collectons pas les données utilisateur que vous saisissez dans les applications présentes sur votre appareil mobile. Ainsi, nous ne lisons pas, n'examinons pas et n'analysons pas vos e-mails ou SMS. Lookout ne collecte pas vos photos ou vidéos, mais peut analyser ces fichiers localement sur votre appareil afin de vous protéger contre certaines menaces qu'ils peuvent renfermer.
- iv. **Données de localisation**. Lorsqu'elle est activée, la fonctionnalité Missing Device de Lookout (qui comprend la fonction Locate and Scream permettant de localiser votre appareil à distance) utilise des Données de localisation pour vous aider à identifier la dernière position connue de votre téléphone si vous le perdez et si sa batterie se décharge complètement. En outre, la fonctionnalité Signal Flare collecte des Données de localisation et les envoie à Lookout dès que votre batterie est faible.

c. Informations collectées par Lookout pour l'Application Lookout Premium Personal

Lookout collecte les mêmes informations que celles détaillées dans la section relative à l'Application Lookout Basic Personal. En plus de ces informations, notre partenaire collecte également des Données de paiement directement auprès de vous pour vous permettre d'accéder à certaines fonctionnalités premium, des Données de contenus Web pour vous permettre d'utiliser la fonctionnalité Safe Browsing, ainsi que des Données sur les alertes de vol pour vous proposer la fonctionnalité Theft Alerts, comme décrit ci-dessus.

- i. **Données de 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 collecter des Données de paiement. Notre fournisseur 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 peut être traité de différentes façons. 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.

- ii. **Données de contenu Web.** Lookout utilise des Données de contenu Web pour vous permettre d'utiliser le service Safe Browsing. 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.
- iii. **Données sur les alertes de vol.** Lorsque la fonctionnalité Theft Alerts 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 e-mail dans les paramètres de votre compte.

d. Informations collectées par Lookout pour l'Application Lookout Premium Plus Personal

Lookout collecte les mêmes informations que celles détaillées dans la section relative à l'Application Lookout Premium Personal. En plus de ces informations, notre partenaire collecte également des Données de protection contre le vol d'identité auprès de vous.

- i. **Données de protection contre le vol d'identité.** Lorsque vous utilisez la fonctionnalité Identity Theft Protection, vous pouvez saisir les Données de protection contre le vol d'identité décrites ci-dessus pour activer certains services de protection de votre identité fournis par notre partenaire tiers CSIdentity (désormais affilié à Experian). Les informations vous concernant collectées et stockées par CSIdentity dépendent des informations que vous avez saisies dans l'Application Personal. CSIdentity peut avoir besoin de communiquer vos Données de protection contre le vol d'identité à des tiers (tels que des sociétés de vérification d'identité, des agences de renseignements sur les consommateurs, des agences d'évaluation du crédit, des sociétés de validation des paiements, des organismes chargés de l'application de la loi, etc.) afin de vous fournir ces services.

e. Informations collectées par Lookout auprès de tiers

Lookout reçoit des Données d'analyse transmises par des tiers, comme décrit ci-dessus.

3. Utilisation de vos informations.

Sauf indication contraire, lorsque nous collectons vos informations, nous les stockons en les associant à votre compte. Veuillez noter que nous avons besoin de certains types d'informations afin de vous permettre d'accéder à nos services. Si vous refusez de nous fournir ces informations ou si vous nous demandez de les supprimer, vous risquez de ne plus pouvoir accéder aux services. 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 aux fins professionnelles et commerciales décrites dans la présente Déclaration. La manière dont nous utilisons vos informations varie selon le type de données, comme décrit ci-dessous :

- a. **Données d'applications.** Nous utilisons ces données pour vous permettre d'utiliser nos services en effectuant des analyses des fichiers d'applications, afin de déterminer si certaines applications présentent un comportement malveillant. Nous rendons également ces données anonymes et nous les agrégeons pour pouvoir connaître la popularité des applications par région et pour réaliser nos analyses des menaces mobiles.

Les données des analyses de menaces mobiles restent anonymes afin de garantir la confidentialité des données. L'association de données client de manière sûre et confidentielle permet à Lookout de mieux appréhender les menaces de sécurité actuelles et d'améliorer ses services.

- b. Données de l'appareil.** Des analyses automatiques de votre appareil peuvent être effectuées à intervalles réguliers pour collecter 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 Personal à détecter et à gérer les menaces sur votre appareil mobile. 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. En plus d'utiliser les informations que vous nous communiquez et celles que nous collectons à partir de votre appareil mobile pour vous délivrer les services Lookout, nous utilisons les informations collectées 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.
- c. Données de protection contre le vol d'identité.** CSIdentity utilise ces informations pour vérifier votre identité et vous fournir les services de protection d'identité souhaités. Si vous souscrivez un abonnement Premium Plus, qui comprend l'assurance contre le vol d'identité, nos partenaires utiliseront vos informations pour vous fournir une assistance et la couverture d'assurance applicable dans le cas où votre identité serait compromise.
- d. Données de localisation.** La fonctionnalité Missing Device de Lookout comprend la fonction Locate and Scream, qui permet de localiser votre appareil à distance à partir de votre compte Personal sur lookout.com. Lookout utilise des Données de localisation pour vous aider à identifier la dernière position connue de votre téléphone si vous le perdez et si sa batterie se décharge complètement. Lorsque vous activez Signal Flare, cette dernière collecte 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 Personal.
- e. Données d'inscription.** Nous pouvons utiliser votre adresse e-mail pour vous informer des annonces de produits et des offres spéciales de Lookout ou de ses partenaires commerciaux. Si vous 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. Nous pouvons utiliser votre adresse e-mail pour envoyer à votre appareil des informations concernant nos services, par exemple pour vous envoyer des notifications liées à la confidentialité ou à la sécurité ou pour vous avertir de toute modification importante des services Lookout.
- f. Données sur les alertes de vol.** Nous utilisons ces informations pour vous proposer nos services d'alertes de vol.
- g. Données de contenu Web.** Safe Browsing est une fonctionnalité conçue pour détecter et signaler les URL dangereuses afin de vous offrir la possibilité de les éviter. Les URL visitées sont rendues anonymes et envoyées à Lookout pour effectuer des contrôles de sécurité. Nous utilisons la liste des URL dangereuses que vous consultez pour vous avertir lorsque vous tentez d'accéder à une URL dangereuse.

4. Divulgence des informations

Cette section décrit la manière dont Lookout peut partager et divulguer vos informations.

- a. Fournisseurs de services tiers et partenaires.** Nous pouvons partager vos informations avec les fournisseurs de services et produits tiers intégrés à nos logiciels qui en ont besoin pour répondre à vos demandes de

produits ou services, pour assurer le bon fonctionnement de nos produits et services et pour analyser les données afin d'améliorer les produits et leurs performances. Par exemple :

- i. Lorsque vous utilisez le service Identity Theft Protection, notre partenaire CSIdentity (désormais affilié à Experian) collecte vos informations pour vous permettre d'utiliser le service. CSIdentity peut alors communiquer vos données à des tiers (tels que des sociétés de vérification d'identité, des agences de renseignements sur les consommateurs, des agences d'évaluation du crédit, des sociétés de validation des paiements, des organismes d'application de la loi, etc.) afin de vous fournir les services demandés. CSIdentity peut également vous fournir des services de surveillance et d'alerte et obtenir des informations et des rapports vous concernant (vous-même ou les autres personnes que vous avez inscrites) afin de fournir les services Identity Protection, y compris des rapports sur l'historique des adresses, les noms, les alias, etc. Nous demandons à CSIdentity et à ses fournisseurs de services d'utiliser les données collectées auprès de vous aux seules fins de fournir des services par le biais de l'Application Lookout Premium Plus.
 - ii. Nous pouvons partager vos informations avec nos revendeurs ou d'autres opérateurs mobiles afin d'assurer la remise de votre achat et le bon fonctionnement des services d'assistance associés et de réaliser certaines fonctions professionnelles.
 - iii. 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. Partenaires de paiement tiers.** Nous pouvons autoriser nos fournisseurs de services à collecter des informations directement auprès de vous pour effectuer des activités de comptabilité, d'audit, de rapprochement des factures et de recouvrement.
- c. Respect de la loi.** 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 d'application de la loi) ; (ii) préserver la sécurité de toute personne, entité ou installation ; (iii) gérer les violations potentielles de notre Déclaration ; (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, de nos employés, des utilisateurs et du 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 e-mail associée à votre compte, sauf (a) si cela nous est interdit ou (b) en cas d'urgence et si vous prévenir pourrait entraîner un risque de blessure ou de décès, ou si cela implique une atteinte potentielle à un mineur. Par ailleurs, rien dans la présente Déclaration 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.
- d. En cas de modification des activités de Lookout.** Nous pouvons également divulguer vos informations à un acheteur ou un acheteur potentiel (ainsi qu'à ses agents et conseillers) dans le cas d'un achat, d'une fusion ou d'une acquisition (confirmés ou potentiels) de toute partie de notre société. Dans ce cas, nous informerons l'acheteur qu'il doit utiliser vos informations uniquement aux fins détaillées dans la présente Déclaration.
- e. Données anonymes et agrégées.** En vue de réaliser des analyses de données, nous rendons anonymes, agrégeons et résumons les données, qui peuvent contenir certaines de vos informations. Nous pouvons rendre publics des rapports élaborés à partir de ces analyses de données afin d'aider les utilisateurs à mieux comprendre les menaces mobiles et le comportement de certaines applications mobiles.
- f. Consentement.** Nous pouvons également partager vos informations avec des tiers dès lors que vous nous y autorisez.

5. Vos choix

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

Vous pouvez mettre à jour les paramètres de votre compte Lookout sur la page « Paramètres » de notre application mobile ou en vous connectant sur notre site Web à l'adresse <https://my.lookout.com/user/login> afin de modifier certains paramètres qui affectent les données qui nous sont communiquées. Pour votre sécurité et votre confidentialité, 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'y apporter des modifications.

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.

6. Conservation des données

Lookout conserve vos informations, y compris vos Données à caractère personnel (telles que définies par le RGPD), uniquement pendant une durée raisonnablement nécessaire pour vous fournir nos produits et services ou pour respecter les exigences légales.

7. Sécurité

a. Responsabilités de Lookout.

Lookout est une société spécialisée dans la sécurité. Nous accordons donc une grande importance à la sécurité de vos données. Lookout s'appuie sur des méthodes de protection physiques, organisationnelles et techniques commercialement raisonnables pour mettre en œuvre des mesures techniques et organisationnelles appropriées en fonction des risques liés au traitement de vos informations. 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 vos Données de localisation) dans l'Application Lookout, nous les chiffons lors de leur stockage et de leur transmission 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 nous prenons connaissance d'une faille de sécurité susceptible de vous affecter, 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.

b. Vos responsabilités.

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-le 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 e-mail 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 informations transmises à un tiers en raison d'une adresse e-mail incorrecte fournie par l'utilisateur.

8. 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 collecter 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 acheté par un parent qui accepte que ces données soient collectées et stockées, comme décrit 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.

9. Transferts de données internationaux

Lookout est une société basée à San Francisco et ses serveurs sont hébergés aux États-Unis. Les données à caractère personnel collectées 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 autonome pour le [Bouclier de protection des données entre l'UE et les États-Unis et entre la Suisse et les États-Unis \(Privacy Shield\)](#), défini par le ministère du Commerce des États-Unis concernant la collecte, l'utilisation et la conservation des Données à caractère personnel provenant des États membres de l'UE, du Royaume-Uni et de Suisse. Ces accords ont été développés pour aider les entreprises à respecter les exigences en matière de protection des données lors du transfert de données à caractère personnel depuis l'Union européenne, le Royaume-Uni et la Suisse vers les États-Unis. Pour en savoir plus sur le Privacy Shield et consulter la liste des entités actuellement certifiées, 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 du fait générateur des dommages.

Nous sommes soumis aux pouvoirs de réglementation et d'exécution de l'U.S. Federal Trade Commission en ce qui concerne les informations personnelles reçues ou transmises dans le cadre des accords du Privacy Shield. Dans certains cas, nous pouvons être amenés à divulguer des informations personnelles pour répondre à des demandes émises par des autorités publiques, y compris pour répondre aux exigences de sécurité ou d'application de la loi nationales.

10. Conditions supplémentaires pour les résidents de l'Espace économique européen (EEE)

a. Base légale de traitement.

Si vous êtes un visiteur de l'EEE, Lookout est le contrôleur de données de vos Données à caractère personnel (telles que définies par le RGPD). La base légale pour la collecte et l'utilisation de vos Données à caractère personnel définie dans la présente Déclaration dépend des Données à caractère personnel concernées et du contexte spécifique dans lequel nous les collectons. Néanmoins, nous ne collectons des Données à caractère personnel auprès de vous uniquement lorsque : (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) l'utilisation de vos Données à caractère personnel est nécessaire pour nos intérêts légitimes ou ceux de tiers (par exemple, pour garantir la sécurité des Services Lookout, exploiter et commercialiser les Services Lookout,

assurer la sécurité des environnements pour notre personnel et des tiers, effectuer et percevoir des paiements, empêcher toute fraude et connaître le client à qui nous fournissons les Services Lookout) ; ou (c) nous sommes autorisés à le faire (par exemple dans le cadre de certaines de nos activités marketing). Une partie du traitement est requise par la législation en vigueur.

b. Vos droits.

Conformément au RGPD, les résidents de l'EEE jouissent des droits décrits ci-dessous. Si vous souhaitez exercer l'un de ces droits, veuillez nous contacter à l'adresse privacy@lookout.com. Nous nous engageons à répondre à votre demande d'accès au plus vite et au plus tard sous 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.

- i. **Accès.** Vous avez le droit de demander une copie des Données à caractère personnel que nous traitons vous concernant. Si vous souhaitez obtenir des copies supplémentaires, nous pouvons les facturer à des frais raisonnables.
- ii. **Rectification.** Vous avez le droit de demander la correction de toute erreur dans les Données à caractère personnel que nous possédons vous concernant (données incomplètes ou erronées).
- iii. **Suppression.** Vous avez le droit de demander la suppression des Données à caractère personnel vous concernant dans certains cas, par exemple lorsque nous n'en avons plus besoin ou si vous décidez de retirer votre consentement (lorsque cela est possible). Outre les droits accordés en vertu de la section ci-dessus intitulée « Vous pouvez accéder à vos paramètres et les mettre à jour », vous pouvez nous contacter à l'adresse privacy@lookout.com pour nous faire part de toute demande.
- iv. **Portabilité.** Vous avez le droit de recevoir les Données à caractère personnel vous concernant que vous nous avez fournies dans un format structuré et couramment utilisé lisible par une machine, et de transmettre ces données à un tiers dans certains cas.
- v. **Objection.** Vous avez le droit de (i) refuser à tout moment le traitement de vos Données à caractère personnel à des fins de marketing direct, et (ii) refuser le traitement de vos Données à caractère personnel lorsque les dispositions juridiques d'un tel traitement sont nécessaires pour nos intérêts légitimes ou ceux de tiers.
- vi. **Restriction.** Vous avez le droit de demander que nous limitions le traitement de vos Données à caractère personnel dans certaines circonstances, par exemple lorsque vous contestez l'exactitude de ces Données à caractère personnel.
- vii. **Retrait de consentement.** Si nous nous appuyons sur votre consentement (ou votre consentement explicite) comme base juridique pour le traitement de vos Données à caractère personnel, vous avez le droit de retirer votre consentement à tout moment. Votre « consentement explicite » est nécessaire si Lookout utilise le consentement comme condition pour traiter légalement des « catégories spéciales de Données à caractère personnel », comme défini dans le RGPD.

Si vous n'êtes pas satisfait de la façon dont nous traitons vos questions concernant nos pratiques de confidentialité, vous pouvez demander une assistance supplémentaire gratuite auprès 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. Vous pouvez également recourir à un arbitrage exécutoire des réclamations. Toutefois, vous devez auparavant : (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. Pour en savoir plus sur le protocole d'arbitrage exécutoire du Privacy Shield, veuillez consulter la page <https://www.privacyshield.gov/article?id=ANNEX-I-introduction>. 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).

11. Contactez-nous pour toute question ou préoccupation

Veuillez contacter notre Responsable de la protection des données à l'adresse privacy@lookout.com ou par courrier à l'adresse Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 28 State Street, 19th Floor, Boston, MA 02109, pour toute question ou remarque concernant la présente Déclaration. Les résidents de l'EEE peuvent également envoyer leurs demandes à l'attention de M. G.J. Schenk, SVP, Florapark 3, 2012 HK Haarlem, Pays-Bas.