Lookout

LIVRE BLANC

Identifier les risques de non-conformité au RGPD dans un monde essentiellement mobile

Comment bénéficier d'une visibilité sur les risques et les menaces mobiles qui pourraient aboutir à des amendes pour non-conformité

« [Les données à caractère personnel doivent] être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). »

RGPD, Article 5, clause 1(f)

Le RGPD est inévitable et aura un impact direct sur la manière dont votre entreprise gère les données à caractère personnel

Le RGPD continue de recevoir beaucoup d'attention de la part des services informatiques et de sécurité d'entreprise, ainsi que de la part de la direction et des conseils d'administration de nombreuses multinationales, ce qui est une très bonne chose. Établi par le Parlement européen, le Conseil européen et la Commission européenne, ce règlement entrera en vigueur le 25 mai 2018. Il a été conçu pour renforcer la protection des données et le respect de la vie privée des personnes résidant dans l'Union européenne (UE). Le RGPD aborde également l'exportation des « données à caractère personnel », c'est-à-dire toute information se rapportant à une personne physique identifiée ou identifiable, en dehors de l'UE.

Définitions	
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (« Personne concernée »)
Personne physique	Être humain
Personne concernée	Toute personne sur laquelle une entreprise dispose de données à caractère personnel

Toute entreprise qui gère des données de personnes physiques en Europe doit se préparer à la conformité RGPD dès aujourd'hui, y compris les nombreuses entreprises américaines établies en Europe ou y proposant des services.

Parallèlement, la technologie mobile est omniprésente. La transformation digitale et mobile a fait des appareils mobiles une infrastructure essentielle aux opérations quotidiennes dans presque toutes les organisations. Cette évolution majeure constitue une menace pour la confidentialité des données à caractère personnel sur mobile. Chaque service et chaque employé de votre entreprise qui a accès à des données à caractère personnel sur les clients, les partenaires ou le personnel peut compromettre la sécurité de ces données en utilisant son appareil mobile, entraînant ainsi une violation du RGPD.

Dans son rapport intitulé Revisit Your Enterprise Mobility Management Practices to Prepare for EU GDPR (Revisitez vos pratiques de gestion de la mobilité d'entreprise pour vous préparer au RGPD de l'UE), le cabinet d'études Gartner explique que « D'ici 2019, 30 % des entreprises courront un risque financier important vis-à-vis des organismes de réglementation suite au non-respect du RGPD pour protéger les données à caractère personnel sur les appareils mobiles ».

Afin d'éviter ce risque et de pleinement respecter le RGPD, les entreprises doivent comprendre le Spectre des risques mobiles et en tenir compte en protégeant les données à caractère personnel des risques liés à la mobilité pouvant compromettre leur capacité à satisfaire aux exigences de conformité.

Téléchargez ici une version imprimable de la Matrice des risques mobiles.

Pourquoi le mobile est un problème pour la conformité RGPD :

La transformation digitale est l'un des principaux facteurs de l'accès accru aux données personnelles visées par le RGPD sur mobile. À mesure que les entreprises s'engagent dans un processus de transformation digitale incluant à la fois le passage au cloud et l'accès intensif aux données via des appareils mobiles, elles augmentent le risque de compromission de ces données, qu'il s'agisse des attaques de logiciels malveillants, de l'exploitation des vulnérabilités ou des fuites de données non malveillantes.

Plus que jamais, les employés ont aujourd'hui l'embarras du choix quant à leur façon de travailler et leur lieu de travail. Ils peuvent, par exemple, choisir leurs appareils, leurs applications et les réseaux à partir desquels accéder aux données et applications d'entreprise. Cela inclut leurs propres appareils et applications, ainsi que ceux dont l'entreprise est propriétaire et qu'elle contrôle. La mobilité a permis aux employés de travailler et d'accéder à leurs données et réseaux professionnels quel que soit l'endroit où ils se trouvent.

Un grand nombre des solutions de sécurité actuelles qu'utilisent les entreprises pour protéger leur matériel et leurs logiciels ne couvre pas tout le spectre des risques mobiles. Les produits hérités développés il y a plusieurs années n'ont pas été conçus pour protéger les points de terminaison mobiles, et même les outils de gestion de la mobilité ne couvrent pas l'ensemble des menaces de sécurité mobiles, des vulnérabilités et des comportements à risque.

À cause de cette faille dans leur sécurité mobile, les entreprises peuvent être victimes d'importantes brèches de sécurité qui se traduisent souvent par l'exposition des données, des pertes financières, des procès et une dégradation de leur image et de leur réputation. Cela ne s'arrête toutefois pas là. Les appareils mobiles font aujourd'hui courir un risque de conformité important aux entreprises. Les mêmes politiques appliquées auparavant aux seuls points de terminaison fixes doivent désormais être appliquées également aux points de terminaison mobiles.

Les entreprises doivent déterminer comment les données peuvent être compromises sur mobile et comprendre comment tant les attaques malveillantes que les fuites de données accidentelles à partir d'applications peuvent compromettre leur conformité et entraîner d'importantes amendes et autres conséquences négatives.

Les entreprises doivent aujourd'hui réfléchir à la manière de garantir la sécurité des données auxquelles accède leur parc d'appareils mobiles. Pour chaque entreprise, la réponse affectera sa capacité à protéger sa propriété intellectuelle et à se mettre en conformité.

*Une enquête en ligne a été réalisée auprès d'un panel de participants potentiels aux États-Unis et au Royaume-Uni. L'enquête s'est déroulée du 5 au 15 septembre 2017. Au total, 2 062 personnes ont participé (en excluant celles qui ont abandonné en cours). Toutes les personnes interrogées étaient âgées d'au moins 18 ans, employées à temps plein dans une entreprise d'au moins 1 000 salariés et travaillaient pour une entreprise avec des employés et/ou des clients/partenaires dans l'Union européenne (à l'exclusion du Royaume-Uni ; en cas de clients/partenaires, l'entreprise devait stocker leurs données à caractère personnel). Parmi les personnes interrogées, 1 000 étaient des décideurs ou impliquées dans le processus décisionnel lié à la sécurité informatique, et occupaient un poste supérieur à celui de stagiaire, simple employé ou analyste/commercial. Les autres personnes interrogées étaient des employés d'entreprises répondant aux mêmes critères que plus haut. L'échantillon a été fourni par Market Cube, un cabinet d'études. Toutes les personnes interrogées ont été invitées à participer à l'enquête par e-mail. La marge d'erreur est de 2,2 %.

Comprendre les menaces et les risques que représente le mobile pour la conformité RGPD

Si de nombreuses entreprises ont déjà commencé le processus de mise en conformité au RGPD, de nombreuses autres n'en sont encore qu'à la phase d'évaluation.

L'un des éléments clés du RGPD est la « protection des données dès la conception » (Privacy by Design), un cadre reposant sur l'intégration proactive de la protection de la vie privée dans la conception même et le fonctionnement des systèmes informatiques, des équipements réseau et des pratiques commerciales.

Le RGPD fait formellement de la protection des données dès la conception une obligation légale pour les entreprises, en promouvant six principes de protection de la vie privée en matière de traitement des données à caractère personnel de l'UE.

Les huit principes du respect de la vie privée

- Licéité
- Loyauté et transparence
- Limitation des finalités
- Minimisation des données
- Exactitude
- Limitation de la conservation
- Intégrité
- Confidentialité

Selon la documentation du RGPD, le principe n°6 stipule que « [les données à caractère personnel doivent] être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».

Ce que de nombreuses entreprises pourraient ne pas pleinement réaliser, même celles qui sont déjà bien avancées dans leur initiative de conformité au RGPD, c'est l'impact de la technologie mobile sur leurs efforts de préparation aux nouvelles règles.

De quelle manière exactement les obligations du RGPD s'appliquent-elles au mobile ?

Traitement des données

Les entreprises doivent savoir à quelles données l'on accède depuis des appareils mobiles, qui accède à ces données, comment cet accès aux données est contrôlé et où vont les données.

Notification des failles

Les entreprises doivent savoir à tout moment quelle est leur visibilité sur les menaces mobiles, comment elles sont informées de ces menaces et comment elles peuvent neutraliser ces menaces dans les meilleurs délais.

Protection des données par défaut

Les entreprises doivent savoir comment trouver l'équilibre du contrôle de la vie privée des utilisateurs finaux et si elles ne collectent pas involontairement des données à caractère personnel qui ne leur sont pas nécessaires.

Un certain nombre de risques mobiles peuvent directement enfreindre le principe n°6 du RGPD

- Des applications malveillantes peuvent s'infiltrer dans les appareils et s'y intégrer si profondément qu'il n'est pas possible de les en supprimer même en réinitialisant les appareils sur leurs paramètres d'usine, créant ainsi une brèche de sécurité pour accéder à distance aux données de manière illicite
- Des méthodes permettent de renforcer la capacité des attaquants à espionner les communications sur l'appareil, pouvant entraîner des pertes de données majeures
- Des applications mobiles peuvent accéder aux listes de contacts et envoyer des données à des serveurs situés en dehors de l'UE
- Des appareils mobiles peuvent être connectés à un réseau compromis par une attaque de type man-in-the-middle, entraînant l'extraction des données de l'appareil

Compte tenu de la prévalence de l'accès aux données depuis des appareils mobiles et de l'utilisation des informations sur les clients, le risque de perte ou de fuite de données est important, que les appareils appartiennent à l'entreprise ou aux employés. Le phénomène du BYOD vient quant à lui encore compliquer les choses. Dans certains pays, de nombreux employés continuent d'apporter leurs propres smartphones et tablettes au travail, ce qui augmente les risques de perte de données, d'obsolescence des correctifs de sécurité et autres problèmes liés à l'utilisation sans distinction des appareils mobiles personnels et professionnels.

Le BYOD est la politique de mobilité la plus courante

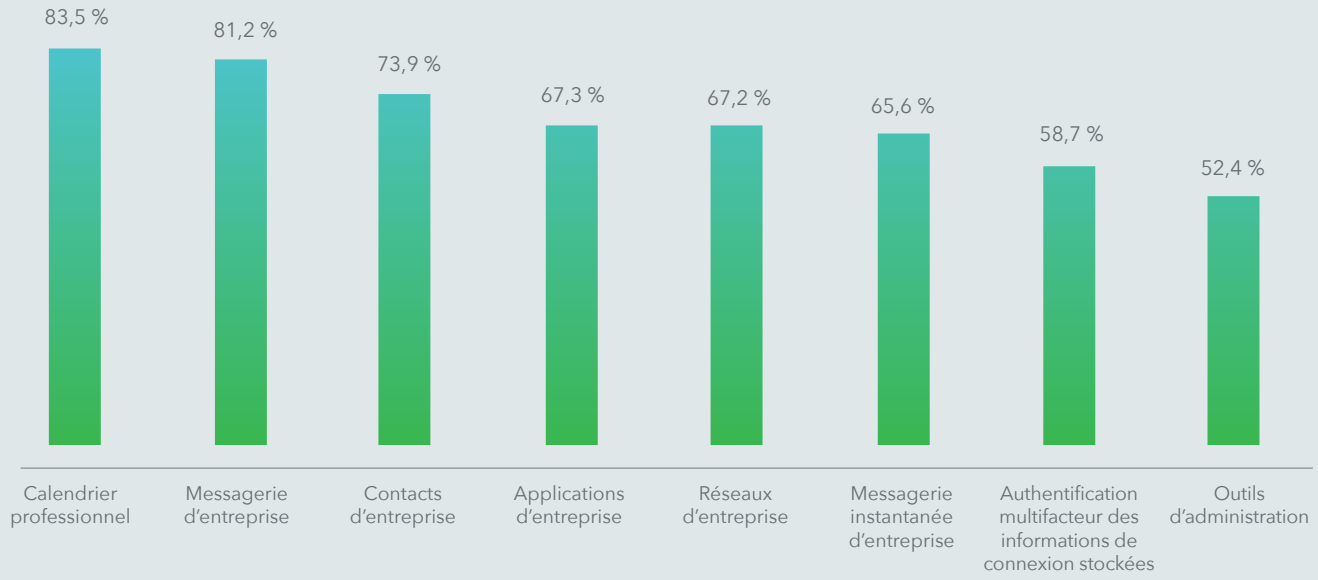
Qu'est-ce qui décrirait le mieux les politiques de mobilité de votre entreprise ?

Le mobile a détrôné l'ordinateur pour l'accès à Internet en novembre 2016. Vos employés passent probablement plus de temps sur leurs appareils mobiles que sur leurs ordinateurs, et consacrent sans doute la plus grande partie de leur temps à travailler avec des applications mobiles plutôt qu'avec un navigateur. La plupart du temps, les gens utilisent ces appareils dans des lieux publics tels que des cafés ou des halls d'hôtel, et comptent sur les réseaux Wi-Fi de tels établissements pour accéder à leurs données d'entreprise. Alors que de nombreuses organisations préfèrent passer au cloud plutôt qu'opter pour des centres de données dédiés, cela peut augmenter les risques de sécurité liés à l'accès aux données.

L'essor conjoint de la mobilité et des services et applications cloud a permis à de nombreuses entreprises de considérablement renforcer la productivité et la collaboration. D'un autre côté, les services informatiques internes et les programmes de sécurité d'entreprise ont en grande partie perdu le contrôle de leurs données et systèmes. Entre la messagerie d'entreprise, les informations de connexion personnelles et professionnelles, l'accès au réseau de l'entreprise et à ses applications, ainsi que les systèmes vidéo et audio embarqués, un smartphone contient toutes les données et autres ressources informatiques nécessaires à la productivité. L'utilisateur mobile d'aujourd'hui peut accéder à un grand nombre de données sensibles et les stocker sur son smartphone, et est fréquemment en déplacement.

De nombreux utilisateurs d'appareils mobiles et les applications mobiles elles-mêmes peuvent faire courir un risque aux données sensibles. Ils peuvent accéder à des données sensibles telles que les données à caractère personnel, charger des données sensibles sur des serveurs externes, enfreindre les réglementations relatives à la souveraineté des données ou encore transférer des données dans des zones à risque. Certaines applications accèdent à des fournisseurs de stockage cloud, des services de réseautage social ou des réseaux de pair à pair, tandis que d'autres utilisent un chiffrement inadéquat lors du stockage ou de l'envoi des données, ou encore présentent des vulnérabilités connues.

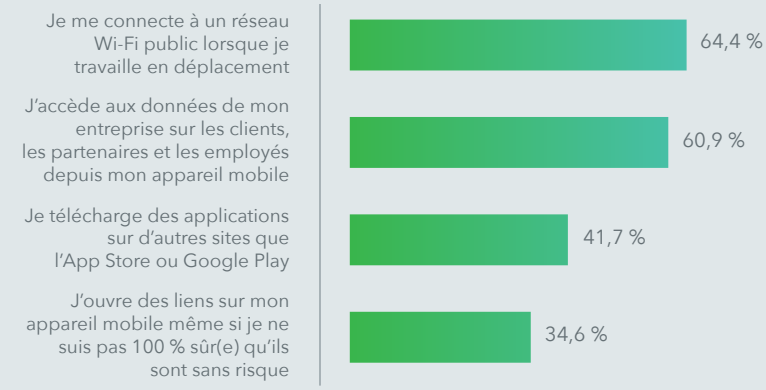
La plupart des employés accèdent à leurs applications de calendrier et de messagerie d'entreprise depuis leur mobile



Avez-vous accès aux éléments ci-dessous sur votre appareil mobile ? Oui/Non

Dans le cadre de leurs efforts de conformité au RGPD, les entreprises doivent déployer des solutions technologiques qui leur permettent de comprendre les capacités et les comportements à risque des applications installées sur les appareils mobiles de leurs employés. Il leur faut pour cela les analyser. Elles ont besoin d'une solution qui les protège des vecteurs d'attaque mobile, tels que les jailbreaks malveillants ou effectués par l'utilisateur final, les vulnérabilités des systèmes d'exploitation, les appareils perdus ou volés, les applications malveillantes ou non conformes, les vulnérabilités applicatives, les fuites de données et les attaques de type man-in-the-middle.

Le comportement des employés fait courir un risque aux données personnelles sur mobile



Parmi les propositions suivantes, quels comportements adoptez-vous sur votre appareil mobile ?

Une fois que les entreprises bénéficient d'une visibilité sur le spectre des risques mobiles, l'étape suivante consiste à établir des politiques pour neutraliser les menaces le plus rapidement possible et atténuer le risque de fuite de données à grande échelle, tout en veillant au respect de la vie privée des utilisateurs finaux. En ce qui concerne l'implémentation de politiques à grande échelle, il est important de retenir qu'un seul moteur de stratégies devrait permettre aux entreprises de spécifier quels types de comportements et autres risques ne sont pas conformes, ce qui leur donnera la possibilité de rapidement se concentrer sur tous les domaines problématiques dans leur parc mobile.

Détecter et stopper les menaces mobiles pesant sur la conformité RGPD

Les entreprises tenues d'observer les exigences de conformité du RGPD doivent se tourner vers des solutions de protection contre les menaces mobiles telles que Lookout Mobile Endpoint Security pour pouvoir bénéficier de la visibilité et des contrôles dont elles ont besoin pour protéger les données à caractère personnel de l'UE et ainsi réduire significativement les risques. Voici de quelle manière une telle solution peut aider les entreprises à se préparer au RGPD :

- **Identifiez rapidement les risques que peuvent présenter les appareils mobiles pour les données à caractère personnel de l'UE.** Lookout Mobile Endpoint Security vous offre la visibilité nécessaire pour rapidement identifier les risques critiques sur le spectre des risques mobiles. Depuis le tableau de bord, vous pouvez accéder aux informations détaillées sur une menace en particulier, une vulnérabilité logicielle ou un comportement et une configuration à risque qui pourraient menacer l'intégrité des données à caractère personnel de l'UE.
- **Implémentez une protection complète basée sur des règles pour neutraliser les risques mobiles à grande échelle.** La solution fournit les contrôles nécessaires pour protéger à grande échelle les données à caractère personnel de l'UE, permettant ainsi aux entreprises de réduire les risques de façon significative. Elles peuvent établir des politiques pour neutraliser les menaces dans les plus brefs délais et atténuer le risque de fuite de données à grande échelle, tout en veillant au respect de la vie privée des utilisateurs.
- **Établissez des politiques d'accès conditionnel basées sur le risque.** L'intégration de Lookout Mobile Endpoint Security avec un système de gestion des appareils mobiles (MDM) permet aux entreprises d'établir des politiques d'accès conditionnel basées sur le risque afin de garantir la sécurité des données d'entreprise. Par exemple, si la solution Lookout détermine qu'un utilisateur a sideloadé une application contenant un logiciel malveillant, elle avertit immédiatement le système MDM que l'appareil n'est plus en conformité et le système MDM peut invoquer une réponse appropriée, comme interdire l'accès de l'appareil à toutes les applications d'entreprise jusqu'à ce que le risque soit éliminé.
- **Préparez-vous aux obligations de notification des failles sous 72 heures requises par le RGPD.** Lookout Mobile Endpoint Security envoie rapidement des notifications aux administrateurs chaque fois que des données sont extraites sans autorisation d'un appareil mobile ou en cas de fuite de données. Ces notifications permettent aux administrateurs d'accéder à des informations détaillées sur le problème dans la console de Lookout et d'en avertir l'autorité de surveillance « dans les meilleurs délais ».
- **Appliquez des garde-fous autour des transferts de données en dehors de l'UE.** La solution permet aux entreprises de savoir quelles applications ne gèrent pas les données au repos ou en transit de manière sécurisée et de connaître la destination des données transférées. Les entreprises peuvent ainsi implémenter des garde-fous autour des données à caractère personnel de l'UE. En ce qui concerne les applications développées en interne, les administrateurs peuvent les importer dans la console où elles seront analysées en vue de détecter d'éventuelles vulnérabilités ou autres comportements à risque.
- **Assurez-vous que votre solution de sécurité mobile adhère aux principes de protection des données dès la conception.** Lookout a développé ses solutions en tenant compte du concept de protection des données dès la conception (Privacy by Design). Avec plusieurs millions d'appareils protégés au monde, l'entreprise possède une solide expérience de la sécurité mobile et sa solution a été conçue pour respecter la vie privée des utilisateurs finaux. Elle propose, par exemple, des contrôles efficaces des données d'ordre privé, avec notamment la possibilité de limiter la collecte de toute information personnelle associée à des utilisateurs ou des appareils gérés.

Ce qui rend la solution de Lookout si particulière et efficace quant à la préparation au RGPD, c'est son impressionnant réseau de capteurs à travers le monde et ses capacités en matière de renseignement sur les menaces (Threat Intelligence). Grâce au succès des produits Lookout pour les points de terminaison personnels et d'entreprise, les clients peuvent compter sur une base de données des menaces et des risques alimentée par plus de 150 millions d'appareils mobiles à travers le monde.

Chaque mois, des millions d'appareils dans plus de 150 pays envoient par télémétrie leurs données de sécurité au Lookout Security Cloud. Lookout peut ainsi suivre l'évolution des acteurs malveillants et détecter les nouvelles menaces, comme le logiciel espion Pegasus. Cet impressionnant ensemble de données mobiles unique au monde offre aux clients les avantages de la précision et du contexte. Il permet en effet aux entreprises de comprendre si un signal ou une caractéristique de menace mobile potentielle est commun, rare ou constitue une véritable anomalie (en se basant sur plus de 50 millions d'applications mobiles uniques à travers le monde) et de suivre sa prévalence en temps réel via le réseau mondial de capteurs de Lookout.

En comprenant parfaitement les exigences du RGPD, y compris ses nombreuses implications pour les appareils mobiles, et en déployant des solutions efficaces pour protéger les données dans leur environnement mobile, les entreprises sont en mesure de se préparer efficacement à ces nouvelles exigences réglementaires.

Il est important de retenir qu'en matière de sécurité et de respect de la vie privée, il est difficile de savoir exactement ce que signifie « être en conformité ». Il existe toujours différents degrés de conformité et rien n'est jamais tout noir, ni tout blanc. Ce qu'une entreprise peut considérer comme une conformité adéquate pourra sembler laxiste ou, au contraire, trop strict à une autre. Tout dépend de la tolérance aux risques de l'entreprise. Par ailleurs, bien qu'aucune solution mobile ne puisse rendre une entreprise « conforme », toute solution de sécurité digne de ce nom devrait couvrir les menaces et vulnérabilités mobiles dont elle pourrait faire l'objet.

Le RGPD redéfinit la manière dont les entreprises doivent gérer et protéger les données à caractère personnel. Il ne s'agit pas d'un nouveau concept, dans la mesure où la plupart des entreprises se sont déjà penchées sur la question d'une manière ou d'une autre. Le temps est toutefois venu d'adapter votre programme de respect de la vie privée pour y inclure votre infrastructure mobile.

Étapes suivantes : bénéficier d'une visibilité sur les menaces mobiles afin d'étendre la conformité RGPD au mobile

Le RGPD redéfinit la manière dont les entreprises doivent gérer et protéger les données à caractère personnel. Il ne s'agit pas d'un nouveau concept, dans la mesure où la plupart des entreprises se sont déjà penchées sur la question d'une manière ou d'une autre. Aujourd'hui toutefois, les entreprises font l'objet d'une pression croissante de la part des pouvoirs publics et des régulateurs en ce qui concerne la protection des données, à laquelle participe le RGPD. Le moment est donc idéal pour adapter votre programme de respect de la vie privée afin d'y inclure votre infrastructure mobile.

Les enjeux de la non-conformité sont extrêmement élevés, notamment d'importantes sanctions financières. Le RGPD indique par exemple que les pénalités pour non-conformité peuvent s'élever jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise en infraction, en fonction de la nature du délit.

Les exigences de la sécurité des données et du respect de la vie privée doivent être étendues à l'environnement mobile, car c'est là que les entreprises effectuent aujourd'hui la plupart de leurs opérations et processus quotidiens. Les menaces de sécurité, les vulnérabilités et les comportements à risque que cela entraîne pour les entreprises peuvent mettre en péril la confidentialité, l'intégrité et la disponibilité des données.

Finalement, la nécessité de se conformer aux nouvelles réglementations offre aux entreprises l'occasion idéale de renforcer leur sécurité globale, y compris la sécurité de leurs écosystèmes mobiles en constante expansion.

Pour en savoir plus sur la façon dont votre entreprise peut étendre la conformité RGPD au mobile, consultez la page www.lookout.com/gdpr.

À propos de Lookout

Lookout est une société de cybersécurité pour un monde axé sur les applications. S'appuyant sur la base de données de code mobile la plus importante au monde, Lookout est la plate-forme de sécurité incontournable pour l'intégrité des appareils mobiles et l'accès aux données. Plus de 100 millions de personnes, des centaines d'entreprises et d'organismes publics, ainsi que tout un écosystème de partenaires tels qu'AT&T, Deutsche Telekom ou encore Microsoft font confiance à Lookout. Lookout a son siège social à San Francisco et possède des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington, DC.