


# Approche Prenez vos appareils personnels (PAP) pour une main-d'œuvre mobile



## TENDANCE TECHNOLOGIQUE

**Selon une étude sur l'approche Prenez vos appareils personnels (PAP) d'A.T. Kearney<sup>1</sup>, « une stratégie et une mise en œuvre bien conçues et fondées sur un mode PAP feront en sorte d'améliorer la productivité et le taux de satisfaction du personnel, sans faire augmenter les coûts ».**

### **Hausse de l'utilisation des appareils personnels au travail**

Plusieurs tendances convergentes ont mené un nombre croissant d'employés à adopter le travail virtuel et le télétravail, qui répondent à divers besoins en matière de mobilité. Les entreprises considèrent habituellement les technologies de l'information (TI) comme des services qui leur appartiennent et qu'elles fournissent grâce à leur infrastructure. La personnalisation des TI vient toutefois changer la donne. Les employés et les consommateurs souhaitent interagir avec les entreprises en utilisant leur propre technologie, comme ils le veulent et quand ils le veulent. Les employés recherchent également la souplesse du travail à distance. Les entreprises plus à l'aise avec des moyens traditionnels pourraient rater l'occasion d'accroître considérablement la satisfaction au travail, la productivité et l'innovation de leurs employés en plus de se priver des possibilités qu'offre le marché. En moyenne, la mise en œuvre d'une approche PAP peut générer une valeur de 350 \$ US par employé mobile<sup>2</sup> parce que 53 % des employés se sentent plus productifs lorsqu'ils utilisent leurs propres appareils<sup>3</sup>.

<sup>1</sup> [www.atkearney.co.jp/documents/10192/585432/Bring+Your+Own+Device.pdf](http://www.atkearney.co.jp/documents/10192/585432/Bring+Your+Own+Device.pdf)

<sup>2</sup> <https://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs>

<sup>3</sup> [https://go.apperian.com/rs/300-EOJ-215/images/Apperian%202016%20Executive%20Enterprise%20Mobility%20Report\\_FINAL\\_20160216.pdf?aliid=16373787](https://go.apperian.com/rs/300-EOJ-215/images/Apperian%202016%20Executive%20Enterprise%20Mobility%20Report_FINAL_20160216.pdf?aliid=16373787)

L'approche PAP permet aux employés d'utiliser leurs propres appareils au travail. L'utilisation d'appareils qui n'appartiennent pas à l'entreprise fera partie intégrante de la stratégie et de l'infrastructure technologiques de l'entité. Dans le cadre de cette approche, les entreprises doivent prendre conscience que le matériel des employés n'est pas soumis à des normes de contrôle aussi strictes que pour le matériel de l'entreprise. C'est pourquoi cette approche soulève des questions sur les aspects suivants :

- Sécurité et contrôle;
- Relations contractuelles;
- Conformité à la réglementation et aux normes du secteur;
- Respect des politiques et des procédures de l'entreprise par les employés.

La gestion des appareils mobiles a pris de l'importance, au même titre que l'adoption croissante du mode PAP par les entreprises, afin de répondre à certains des problèmes auxquels ces dernières font face. Tout comme pour les outils traditionnels de gestion des actifs TI, les solutions de gestion des appareils mobiles offrent aux entreprises la capacité de gérer les politiques, les stocks et la sécurité relativement aux appareils mobiles personnels de leurs employés.

Dans le mode PAP, la propriété des appareils est transférée aux employés, mais l'entreprise demeure tout de même responsable de protéger ses données et de s'assurer que l'utilisation des appareils personnels répond à ses normes de contrôle.

## Importance

Étant donné que les employés adoptent la mobilité en milieu de travail, les appareils mobiles deviennent un trésor d'informations d'entreprise. Par conséquent, les CPA occupant des fonctions de gestion des risques ou de surveillance doivent aider leur entreprise à protéger les biens et la propriété intellectuelle en s'assurant de la sécurité et du contrôle adéquat des données. Selon une étude récente, plus de 60 % des propriétaires de petites entreprises estiment que le risque d'atteinte à la sécurité des données est plus élevé lorsque les employés travaillent à distance, et 40 % des hauts dirigeants et propriétaires d'entreprise jugent que l'erreur humaine ou la perte accidentelle est la cause principale d'atteinte à la sécurité des données<sup>4</sup>.

Puisque les pertes accidentelles d'appareils mobiles sont particulièrement courantes, les entreprises ont établi des politiques et des procédures et adopté des logiciels visant les appareils qu'elles détiennent afin d'atténuer le risque de perte de données. Mais qu'en

4 [www.shredit.com/en-us/about/press-room/press-releases/shred-it-study-exposes-employee-negligence](http://www.shredit.com/en-us/about/press-room/press-releases/shred-it-study-exposes-employee-negligence)

est-il des appareils personnels? Les entreprises qui veulent assurer la sécurité d'appareils personnels et exercer un contrôle efficace sur ceux-ci sont confrontées à d'importants nouveaux défis.

## Avantages et considérations pour les entreprises

Voici quelques-uns des avantages de la stratégie PAP pour les entreprises :

- Réduction des coûts liés au matériel, au soutien et aux télécommunications;
- Amélioration de la flexibilité en milieu de travail entraînant un taux plus élevé de satisfaction et de bonheur chez les employés;
- Amélioration de la productivité des employés puisqu'ils connaissent bien leurs propres appareils et qu'ils sont à l'aise de les utiliser;
- Réactivité accrue des employés, car ils sont généralement toujours en possession de leurs appareils personnels.

Toutefois, les organisations qui envisagent d'implanter une stratégie PAP doivent élaborer des politiques et des procédures détaillées sur l'utilisation d'appareils personnels. De telles politiques doivent comprendre des directives précises sur la protection, l'utilisation, le stockage, la maintenance, l'archivage et la destruction des données de l'entreprise. Les solutions de gestion des appareils mobiles élaborées par des tiers (p. ex. : IBM MaaS360, Microsoft Intune, SOTI MobiControl, Duo Beyond, etc.) peuvent aider les entreprises à gérer les appareils personnels des employés. Les organisations doivent aussi songer à offrir du soutien et des conseils appropriés sur les pratiques exemplaires en matière de sécurité afin d'aider les employés à déceler et à résoudre les problèmes liés à l'utilisation de leurs appareils personnels pour le travail.

Le tableau suivant présente un résumé des risques et des stratégies d'atténuation pour les entreprises adoptant une approche PAP.

| Risques   | Stratégies d'atténuation des risques  |
|---|---|
| <p><b>L'entité ne dispose pas de politiques, de procédures ou de directives particulières sur les problèmes relatifs au mode PAP pour guider les employés et les autres personnes travaillant dans un contexte PAP.</b></p> | <ul style="list-style-type: none"> <li>• Élaborer et mettre en œuvre des politiques et procédures complètes et efficaces sur le mode PAP et surveiller leur application.</li> <li>• Appuyer les politiques et procédures par une orientation et une formation adéquates.</li> </ul> |

| Risques  | Stratégies d'atténuation des risques  |
|--|---|
| <p><b>Les employés peuvent se servir de leurs appareils personnels pour stocker des renseignements confidentiels ou privés de l'entreprise, ce qui accroît les possibilités d'utilisation abusive, de perte ou de divulgation.</b></p>   | <ul style="list-style-type: none"> <li>• Mettre en œuvre des politiques qui limitent le stockage de tels renseignements sur les appareils personnels non sécurisés.</li> <li>• Créer un « profil d'entreprise » sur l'appareil personnel de manière à limiter le stockage de données ou à séparer les données entre les applications personnelles et celles de l'entreprise.</li> <li>• L'ouverture d'une session doit inclure la synchronisation automatique des données avec les bases de données de l'entreprise.</li> <li>• Si les appareils sont connectés en permanence, configurer des sauvegardes périodiques en mode tirer ou pousser.</li> </ul>  |
| <p><b>Incapacité ou difficulté à protéger les données de l'entreprise sur des appareils personnels perdus ou volés.</b></p>  | <p>Adopter une politique qui assujettit tous les appareils contenant des données de l'entreprise aux politiques de sécurité de l'information de l'entreprise ainsi qu'aux outils de surveillance et aux examens périodiques de la direction. Voici quelques exemples de politiques de sécurité qui pourraient être exigées :</p> <ul style="list-style-type: none"> <li>• Installation de solutions de gestion des appareils mobiles afin de favoriser la gestion et la mise en application des politiques et des règles de sécurité;</li> <li>• Chiffrement et sauvegarde régulière des données de l'entreprise sur l'appareil;</li> <li>• Possibilité pour l'entreprise d'effacer les données à distance en cas de perte ou de vol de l'appareil;</li> <li>• Utilisation obligatoire d'un mot de passe complexe devant être modifié régulièrement et activation d'une authentification multifactorielle.</li> </ul> |
| <p><b>L'entité doit traiter les questions de contrôle et de propriété des données (les données appartiennent-elles à l'entreprise ou à la personne et quelles sont les obligations juridiques et contractuelles de l'entité en matière de protection de ces données?).</b></p> | <ul style="list-style-type: none"> <li>• Élaborer et mettre en œuvre des politiques et procédures complètes et efficaces en matière de contrôle et de propriété des données sur un appareil personnel, puis surveiller leur application.</li> <li>• Élaborer et mettre en œuvre des contrôles sur le classement des données d'entreprise et appliquer les mécanismes de protection connexes aux données liées au mode PAP.</li> <li>• Élaborer des politiques et des procédures sur l'examen et l'effacement des données et des applications de l'entreprise pour les employés qui quittent leur emploi.</li> </ul>   |

| Risques   | Stratégies d'atténuation des risques   |
|---|--|
| <b>Les employés ou les sous-traitants peuvent s'abonner à un service de sauvegarde commercial et enfreindre involontairement des lois et des ententes en incluant l'information de l'entreprise dans ces sauvegardes.</b>   | <ul style="list-style-type: none"> <li>• Configurer les appareils de façon à exclure les fichiers de l'organisation d'une sauvegarde commerciale lancée par l'employé.</li> <li>• Créer un « profil d'entreprise » compartimenté sur l'appareil personnel de manière à limiter le stockage de données ou à séparer les données entre les applications personnelles et celles de l'entreprise, puis empêcher le service de sauvegarde utilisé par l'employé d'accéder aux données d'entreprise.</li> </ul>  |
| <b>Les ressources TI feront l'objet de demandes accrues pour un large éventail d'appareils personnels.</b>  | <ul style="list-style-type: none"> <li>• Établir une liste d'appareils autorisés et pris en charge que les employés peuvent apporter au travail.</li> <li>• Définir clairement le niveau de soutien offert pour les appareils personnels et limiter ce soutien aux problèmes liés à l'utilisation commerciale seulement.</li> </ul>  |
| <b>L'utilisation accrue des appareils mobiles et l'intégration de ces derniers dans les processus d'affaires créent de nouvelles préoccupations concernant la gestion des appareils, le développement d'une plateforme de mobilité et les capacités de gestion des données mobiles.</b> | <ul style="list-style-type: none"> <li>• Établir des procédures afin d'appliquer les politiques relatives aux appareils mobiles.</li> <li>• Sensibiliser les utilisateurs à la sécurité, à l'utilisation et à d'autres politiques et procédures connexes afin qu'ils comprennent clairement les attentes et les limites entourant l'utilisation appropriée des appareils mobiles en milieu de travail.</li> <li>• Mettre en œuvre des solutions technologiques, telles que la gestion des appareils mobiles, pour soutenir les politiques et procédures; vérifier la configuration des appareils par rapport aux normes de l'entreprise; et effectuer des vérifications périodiques ou permanentes et, le cas échéant, modifier ou mettre à jour les paramètres avant d'autoriser la session à se poursuivre.</li> </ul> |

## Conclusion

La demande de mobilité en milieu de travail est appelée à s'accroître. Les entreprises doivent se doter de stratégies pour aider leurs employés à réussir dans ce nouvel environnement de travail et, pour ce faire, la mise en place d'une stratégie PAP efficace est un bon point de départ.

La présente publication s'inscrit dans la série Tendance technologique, qui porte sur les grandes tendances du domaine touchant le milieu comptable. Les documents de cette série sont disponibles sur notre site Web.

### AVIS DE NON-RESPONSABILITÉ

Le présent document, préparé par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité. CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de ce document.

© 2019 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d'auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

Pour demander cette autorisation, veuillez écrire à [permissions@cpacanada.ca](mailto:permissions@cpacanada.ca).