Fiche pratique

BYOD : quelles sont les bonnes pratiques ?

19 février 2015

Avec le développement du BYOD, on assiste à un effacement progressif des frontières entre vie professionnelle et personnelle. La CNIL rappelle les bonnes pratiques permettant de concilier sécurité des données de l'entreprise et protection de la vie privée du salarié connecté.

1 Qu'est ce que le « Bring Your Own Device » (BYOD) ?

L'acronyme « *BYOD* » est l'abréviation de l'expression anglaise « *Bring Your Own Device* » (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC) qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.

Il peut s'agir par exemple d'un salarié qui, pour se connecter au réseau de l'entreprise, utilise par exemple un ordinateur, une tablette ou son smartphone personnel.

2 Les outils personnels ne peuvent être utilisés qu'à titre subsidiaire dans un cadre professionnel

Le droit du travail impose à l'employeur de fournir à ses employés les moyens nécessaires à l'exécution de leurs tâches professionnelles.

L'utilisation d'outils informatiques personnels à des fins professionnelles ne permet pas de s'affranchir de cette obligation.

3 La sécurité des données

L'employeur est responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, **mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.**

Les risques contre lesquels il est indispensable de se prémunir vont de l'atteinte ponctuelle à la disponibilité, l'intégrité et la confidentialité des données, à la compromission générale du système d'information de l'entreprise (intrusion, virus, chevaux de Troie, etc.).

4 Comment limiter les risques pour la sécurité des données ?

- **Identifier les risques**, en tenant compte des spécificités du contexte (quels équipements, quelles applications, quelles données ?), et les estimer en termes de gravité et de vraisemblance.
- **Déterminer les mesures à mettre en œuvre et les formaliser dans une politique de sécurité.**

Par exemple :

- cloisonner les parties de l'outil personnel ayant vocation à être utilisées dans un cadre professionnel (création d'une « bulle de sécurité ») ;
- contrôler l'accès distant par un dispositif d'authentification robuste de l'utilisateur (si possible à l'aide d'un certificat électronique, d'une carte à puce…) ;
- mettre en place des mesures de chiffrement des flux d'informations (VPN, HTTPS, etc.) ;
- prévoir une procédure en cas de panne/perte du terminal personnel (information de l'administrateur réseau, mise à disposition d'un équipement alternatif professionnel, effacement à distance des données professionnelles stockées sur le terminal personnel) ;
- exiger le respect de mesures de sécurité élémentaires telles que le verrouillage du terminal avec un mot de passe suffisamment robuste, renouvelé régulièrement (8 caractères avec des lettres minuscules, majuscules, des chiffres et des caractères spéciaux) et l'utilisation d'un antivirus à jour.

- **Sensibiliser les utilisateurs** aux risques, **formaliser les responsabilités** de chacun et **préciser les précautions à prendre dans une charte** ayant valeur contraignante.
- **Subordonner l'utilisation des équipements personnels à une autorisation** préalable de l'administrateur réseau et/ou de l'employeur.

5 Quelles garanties pour la vie privée ?

La sécurité du système d'information de l'entreprise doit être conciliée avec le respect de la vie privée des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle.

Par exemple, il n'est pas possible de prévoir des mesures de sécurité ayant pour objet ou effet d'entraver l'utilisation d'un smartphone dans un cadre privé, au motif que cet équipement peut être utilisé pour accéder aux ressources de l'entreprise (interdire la navigation sur internet, le téléchargement d'applications mobiles).

De telles restrictions pourraient difficilement être considérées comme justifiées par la nature de la tâche à accomplir et proportionnées au but recherché.

De la même manière, l'employeur ne peut accéder à des éléments relevant de la vie privée stockés dans l'espace personnel de l'équipement (liste des sites internet consultés, photos, films, agenda, annuaire).

Si l'employeur peut prévoir un effacement à distance de la partie du terminal personnel spécifiquement dédiée à l'accès distant aux ressources de l'entreprise, il ne peut en revanche s'arroger le droit d'effacer à distance l'ensemble des données présentes sur le terminal de l'employé.

6 Quelle formalité ?

Lorsque l'employeur a effectué une déclaration normale de gestion du personnel incluant le traitement des données personnelles pour assurer la sécurité et le bon fonctionnement des systèmes d'information, il n'y a pas lieu de procéder à une nouvelle déclaration du fait du recours au BYOD. C'est le cas aussi s'il a désigné un Correspondant informatique et libertés.

La norme simplifiée n°46 n'est pas applicable car elle concerne uniquement les moyens informatiques mis à disposition par les employeurs, ce qui n'est pas le cas du BYOD par définition.

Recourir au BYOD ne change pas les formalités auxquelles les traitements métiers sont soumis (demande d'avis, demande d'autorisation ou déclaration

selon les cas).

7 Les textes de référence

Le Code du travail :

- Article L. 1121-1 (protection des droits fondamentaux des salariés)
- Article L. 1222-4 (information des salariés)
- Article L. 2323-32 (information du comité d'entreprise quant aux outils permettant un contrôle de l'activité des salariés)

Le Code civil :

- Article 9 (protection de l'intimité de la vie privée)

La loi du 6 janvier 1978 dite loi « Informatique et libertés »:

- Article 2
- Article 34 (sécurité des données)

Documents utiles en complément :

- **BYOD - Éléments de réflexion pour gérer les risques, Club EBIOS, 2014**
- **Les terminaux personnels en Entreprise - FAQ, Forum des compétences, 2014**

RETOUR