GS Days
Les journées francophones de la sécurité

24 mars 2015, Paris

Pinsent Masons

Les usages de la mobilité au sein de l'entreprise (du « BYOD » au « COPE »)

Diane Mullenex et Guillaume Morat

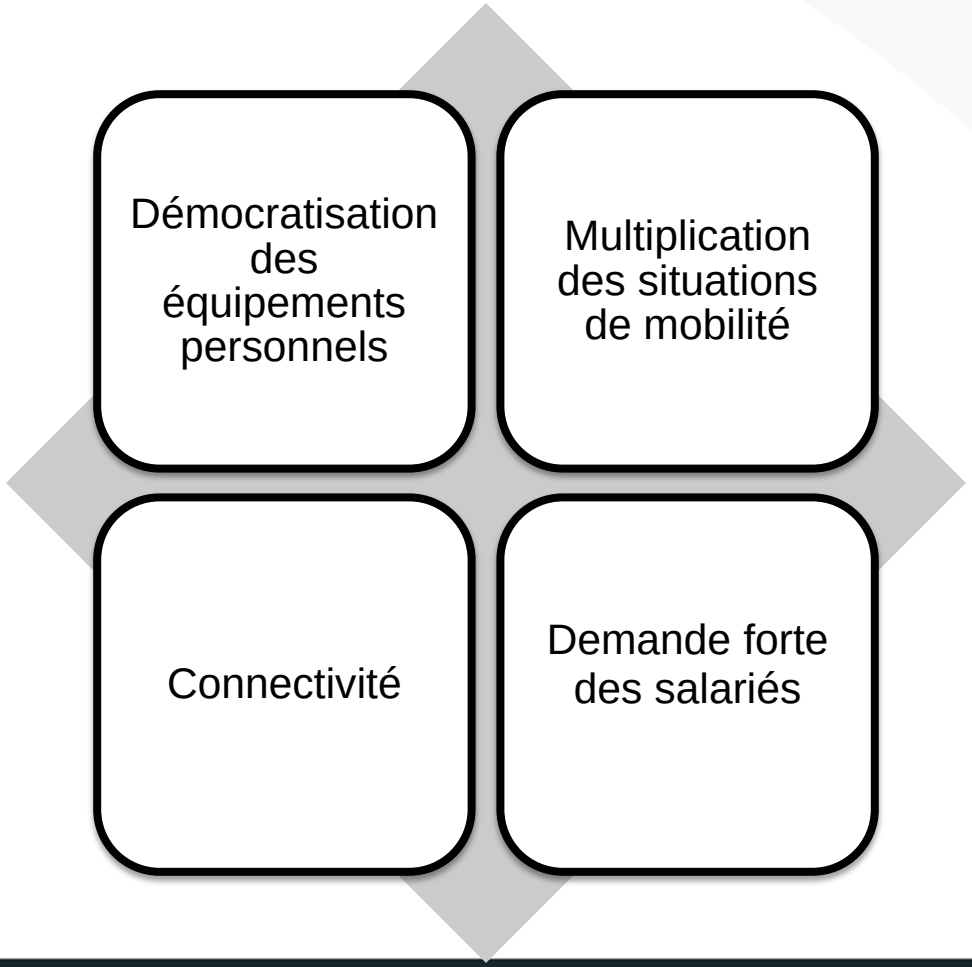
Pinsent Masons France LLP

Pinsent Masons

I. Contexte et pratiques

Pinsent Masons

La naissance du BYOD



Pinsent Masons

La naissance du BYOD

- Extrait Google Trends : “BYOD”

Pinsent Masons

Le BYOD en chiffres

- 78% des entreprises françaises autorisent (ou n'interdisent pas) l'usage d'appareils personnels à des fins professionnelles

- 74% des entreprises françaises qui autorisent leurs employés à utiliser des appareils personnels au travail constatent des retombées positives sur la productivité et l'efficacité des employés

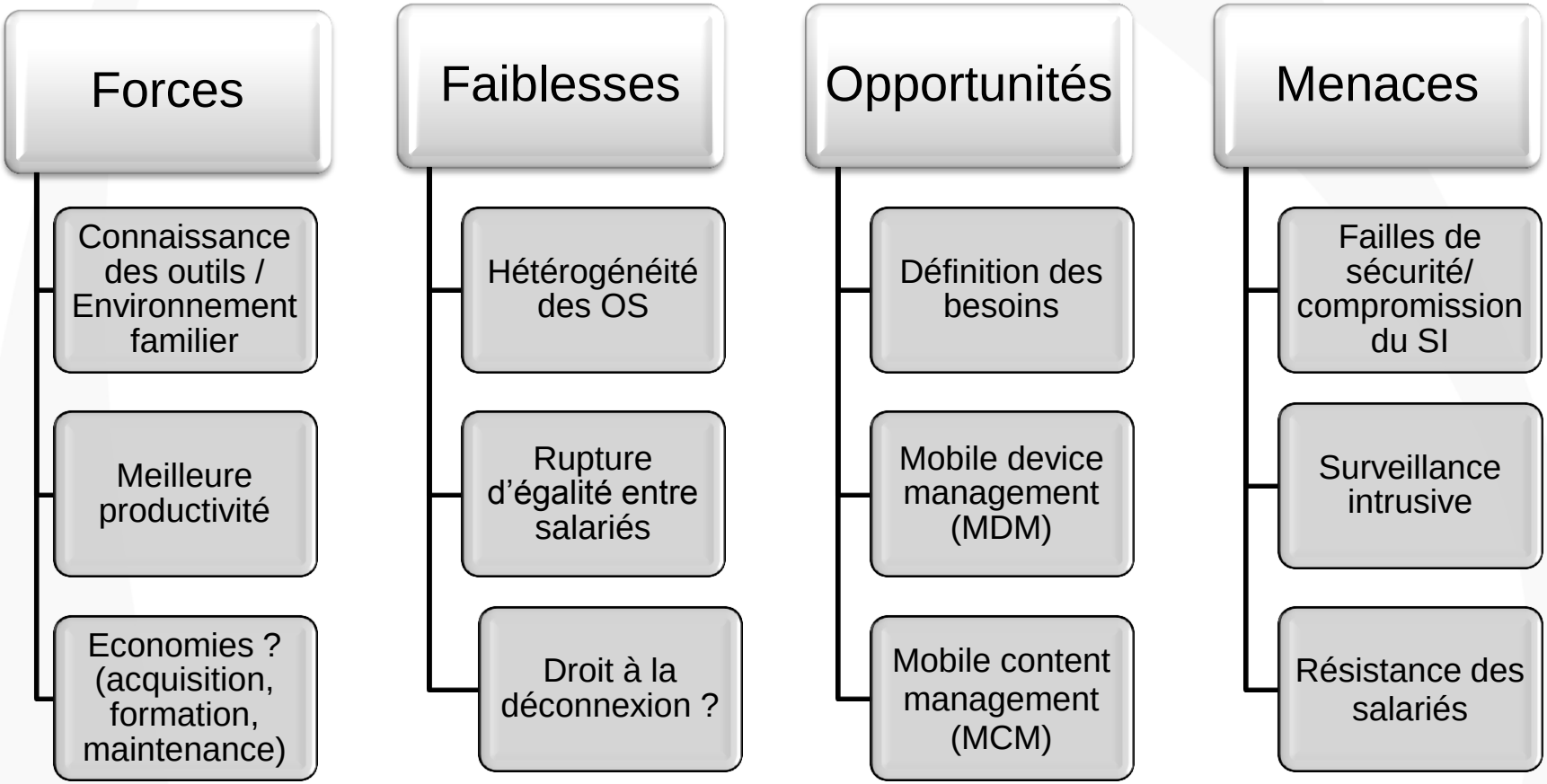
- Seules 26 % des entreprises disposent de politiques et de moyens de sécurité pour gérer les appareils personnels des salariés utilisés à des fins professionnelles

Pinsent Masons

“ Ils sont passés au BYOD …”

- Ford : programme BYOD en mai 2007
- Revevol: programme CYOD en 2007
- Cisco : programme BYOD à grande échelle
- Citrix : enveloppe budgétaire de 2100$ à chaque employé désirant intégrer le programme BYOD
- IBM : programme BYOD en 2010
- Colgate-Palmolive : programme BYOD en mars 2011
- Volvo : programme BYOD en septembre 2011

Pourquoi le BYOD ?



Pinsent Masons

Les solutions techniques – les approches

- Approche n° 1 : ne pas autoriser le stockage sur le terminal (accès classique : webmails, etc.)

- Approche n° 2 : virtualiser sur le même matériel un environnement professionnel et un environnement personnel

La définition des besoins

- Quels équipements ?
  - Ordinateur portables
  - Téléphones portables
  - Tablettes
- Quels systèmes d'exploitation ?
  - PC : Microsoft Windows, Mac OS, Linux
  - Mobile : iOS, Android, Windows Phone, BlackBerry OS
- Quelles applications ?
  - Applications standards (messagerie, base de contacts, intranet, etc.)
  - Applications métiers
- Quelle population ?
  - Salariés / Prestataires
  - Cadres / Commerciaux / Supports

Le choix du modèle

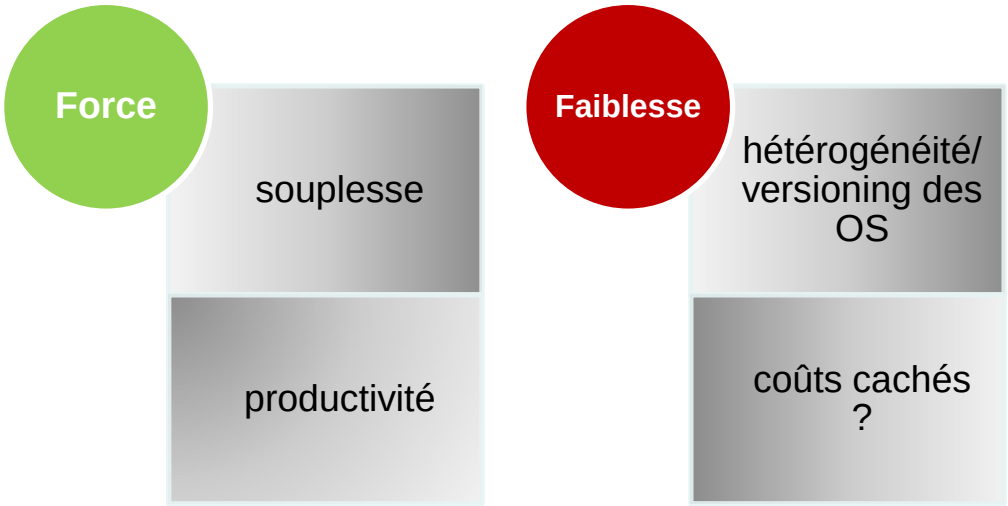
BYOD ou Bring your own device

CYOD ou Choose Your Own Device

COPE ou Corporate Owned, Personally Enabled

Qu’est ce que le BYOD ?

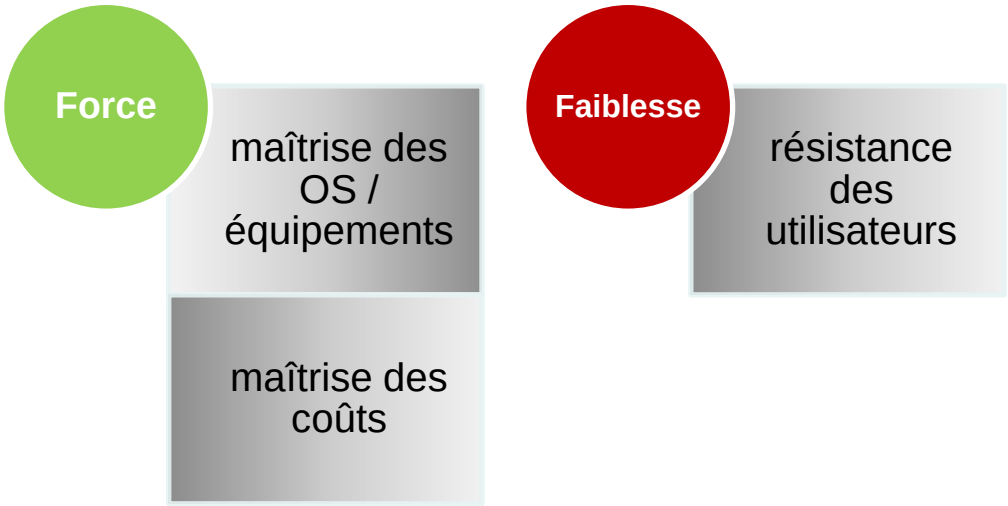
- Le BYOD ou Bring Your Own Device (en français « AVEC » ou Apportez votre équipement personnel de communication): le salarié utilise son propre appareil pour son usage professionnel



Pinsent Masons

Qu’est ce que le CYOD ?

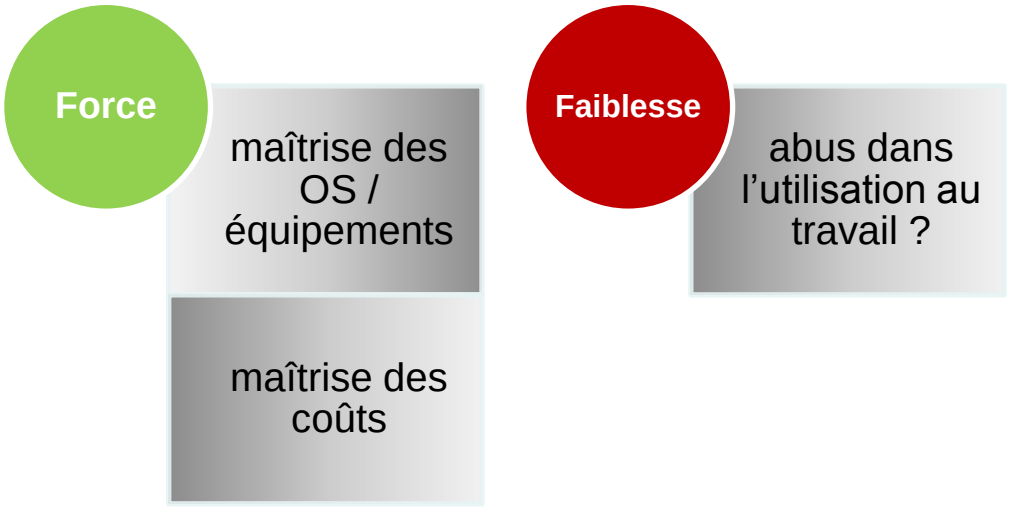
- Le CYOD ou Choose Your Own Device :
  - L’entreprise finance les appareils utilisés
  - Le salarié choisit le modèle d’appareil parmi une liste déterminée par l’entreprise



Pinsent Masons

Qu’est-ce que le COPE ?

- Le COPE ou Corporate Owned, Personally Enabled :
  - L’entreprise finance les appareils utilisés
  - L’entreprise choisit le modèle
  - Le salarié peut utiliser librement l’appareil pour son usage personnel



Pinsent Masons

Et le BYOCL ?

- Le BYOCL ou Bring Your Own Connected Life :
  - Utilisation d'outils connectés pour analyser le comportement des salariés
  - Permet au salarié de disposer d'outils innovants
  - Exemple : montres connectées afin de rappeler les rdv, capteur de stress…(Big data)

II. Panorama des risques juridiques pour les entreprises

Pinsent Masons

Cinq thématiques

- Droit du travail
- Sécurité des SI
- Informatique et Libertés
- Contrats
- Droit fiscal

Le BYOD et le droit du travail

Pinsent Masons

Le contrôle du salarié par son employeur

- **Un employeur peut-il contrôler l'activité de ses salariés au travail en consultant les appareils mis à leur disposition ?**

  - Le salarié a droit au respect de sa vie privée même sur son lieu de travail (« vie privée résiduelle »)

  - L'employeur ne peut prendre connaissance des documents identifiés comme personnels qu'en présence du salarié sauf risque ou évènement particulier

  - Les autres documents peuvent être consultés par l'employeur en l'absence du salarié

Le contrôle du salarié par son employeur

- **Les informations stockées sur l'appareil personnel d'un salarié sont-elles personnelles?**

- Le cas de la clé USB personnelle d'un salarié connectée à son poste de travail :
  - Elle est présumée être utilisée à des fins professionnelles (critère : connexion à un outil professionnel)
  - Les documents qu'elle contient peuvent être consultés par l'employeur en l'absence du salarié s'ils ne sont pas identifiés comme personnels

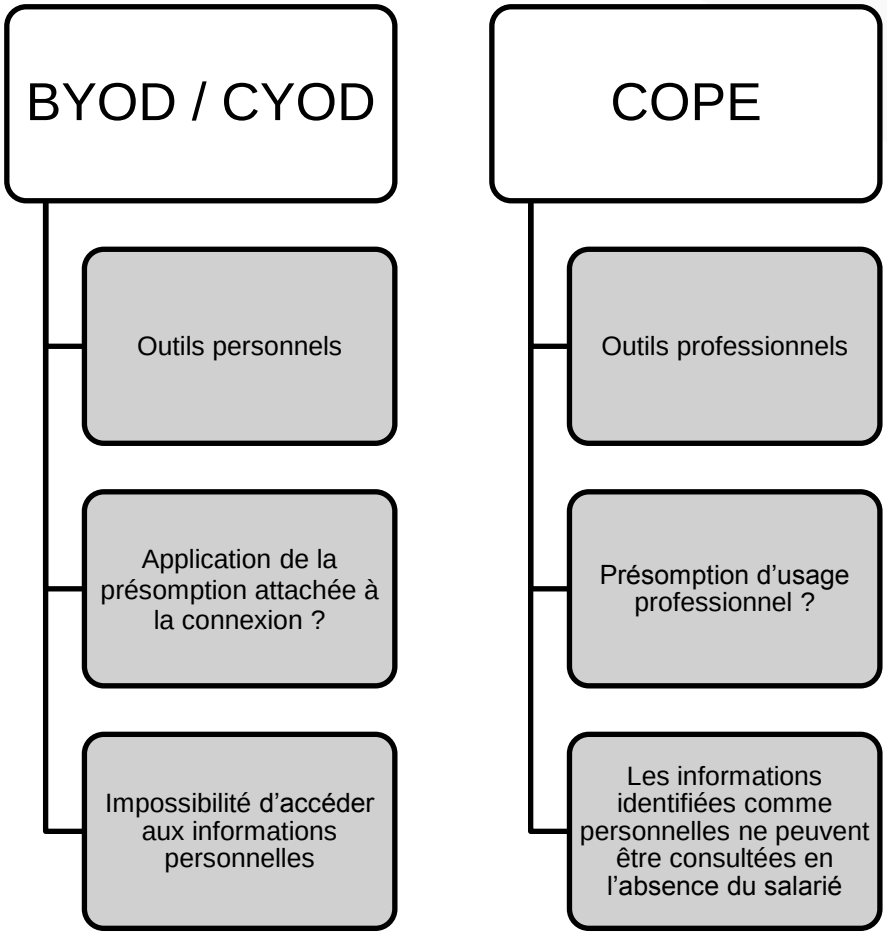
- Le cas du dictaphone personnel d'un salarié utilisé pour enregistrer les conversations au sein de la société :
  - L'employeur ne peut le consulter qu'avec la présence du salarié

Le contrôle du salarié par son employeur

- **Le cas des SMS personnels stockés sur un téléphone professionnel ?**

- Les contenus d'un outil mis à disposition par l'employeur sont présumés professionnels
- Si les SMS ne sont pas identifiés « personnels », ils peuvent être consultés par l'employé sans la présence du salarié

Et en pratique ?



Pinsent Masons

Le temps de travail effectif

- Risque d'une utilisation abusive des appareils mis à la disposition des salariés sur leur temps de travail

➢ Comment comptabiliser les heures travaillées sur un terminal personnel ?

  - Les heures supplémentaires effectuées par un salarié ne sont considérées comme des heures supplémentaires que si elles ont été effectuées à la demande de l'employeur ou avec l'accord implicite de l'employeur;

  - Ainsi, le salarié qui effectue des heures supplémentaires avec son terminal personnel de sa propre initiative, en dehors de toute demande de l'employeur, ne pourra pas être rémunéré à ce titre.

  - Quid du « droit à déconnexion » ?

Acceptation par les salariés

- Lien de subordination hiérarchique salarié / employeur :
  - Quid résistance des salariés à l'utilisation du BYOD ?
  - Quid des salariés qui ne disposent pas de terminal personnel ?
- 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.
- Mise en œuvre d'une politique BYOD généralisée délicate ?

Le BYOD et la sécurité des données

Pinsent Masons

La sécurité des données

- L’employeur n’a pas la maitrise sur l’usage de l’appareil du salarié
  - divulgation de données ou informations confidentielles
  - intrusion sur le système sur le système du salarié
  - compromission du SI

La sécurité des données

- Qui est responsable en cas de perte ou de vol de l'appareil du salarié entrainant la perte de données ?

- Principe de responsabilité de l'employeur du fait de ses salariés vis-à-vis des tiers

- Le salarié est tenu à une obligation de loyauté et de confidentialité et sa responsabilité pourra être engagée envers son employeur

La sécurité des données

- Norme à venir ? Référentiel ISACA sur l'audit du BYOD

- Aux Etats-Unis, 21% des sociétés affirment procéder à l'effacement à distance des données lorsque leur employé quitte la société ; quels sont les risques de responsabilité pour les sociétés ?

Le BYOD et la protection des données à caractère personnel

Pinsent Masons

La protection des données personnelles

- Lorsqu'une entreprise collecte des données personnelles sur ses clients ou ses salariés, elle est tenue de garantir la sécurité de ces données (art. 34 de la loi 78-17).

- Les risques :
  - Perte de contrôle sur la diffusion des données
  - Installation de logiciels malveillants sur l'appareil personnel

La protection des données personnelles

- CNIL – Fiche pratique sur le BYOD (février 2015)
  - Le recours au BYOD ne change pas le régime des formalités applicables :
  - Soit déclaration normale de gestion du personnel incluant le traitement des données personnelles pour assurer la sécurité et le bon fonctionnement des systèmes d'information
  - Soit inscription au registre des traitements en cas de présence d'un CIL

Les risques d’atteinte à la réputation

- En cas de fuite de données personnelles, les opérateurs de communications électroniques doivent le notifier à la CNIL qui pourra ordonner d’en informer les personnes concernées

- Cette obligation devrait être étendue d’ici à 2017, lors de l’entrée en vigueur du projet de règlement européen sur la protection des données personnelles

Le BYOD et le droit des contrats

Pinsent Masons

Le respect des contrats

- Licences d'utilisation
  - L'utilisation par l'employé de ses logiciels acquis à titre personnel ne permet pas nécessairement l'usage professionnel
  - L'utilisation par l'employé à titre personnel des logiciels sous licence professionnelle n'est pas nécessairement permise
  - Le nombre d'utilisateurs permis par la licence professionnelle peut être limité

Le BYOD et le droit fiscal

Pinsent Masons

Les avantages fiscaux

- Régime du télétravail applicable au BYOD ?
  - Si l'employeur rembourse des frais dépensés par l'employé, il peut prétendre à une déduction de l'assiette de ses cotisations
  - Frais générés par le télétravail sont réputés être des dépenses professionnelles et déductibles
  - Ex : en cas d'achat de matériel par le salarié, l'employeur peut déduire jusqu'à 50% de la dépense réelle remboursée au salarié sur justificatifs

III. La maîtrise des risques juridiques

Pinsent Masons

Droit du travail

- A1 : Mise en place d'une charte informatique / charte BYOD
  - Contrôle, conditions d'accès
  - Procédure d'alerte (vol, perte, logiciels malveillants, etc.)
  - Encadrement des usages
  - Sanctions
- A2 : Information des IRP
- A3 : Accompagnement dans les démarches

Sécurité des données

- A1: Politique de sécurité - Définition des mesures de sécurité (ex.)
  - 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 (verrouillage du terminal avec un mot de passe suffisamment robuste, renouvelé régulièrement, utilisation d'un antivirus à jour etc.)

Sécurité des données

- A2 : Choix de solutions MCM / MDM
- A3 : Sensibilisation du personnel
- A4 : Police d’assurance

Protection des données personnelles

- A1 : Mise en place de moyens renforcés de contrôle des accès
- A2 : Formalités CNIL

Respect des contrats

- A1 : Audit des contrats de licence
- A2 : Informations liées aux logiciels piratés ou dont la licence est incompatible avec un usage professionnel

Pinsent Masons

For a full list of our locations around the globe please visit our websites:

www.pinsentmasons.com

www.Out-Law.com