

Sécurité dans l'entreprise

Nouvelles technologies

Quelles responsabilités ? Quels risques ?

Christiane Féral-Schuhl
Avocat Associé

9, rue Royale, 75008 Paris

Tél : 33 (0)1 70 71 22 00 - Fax : 33 (0)1 70 71 22 22 - E-mail : contact@feral-avocats.com

www.feral-avocats.com

1. Atteintes en provenance de l'extérieur/de l'intérieur

- ❑ Mesures de protection technique
 - ✓ pare-feu, anti-virus...
- ❑ Veille sécuritaire permanente
 - ✓ audits, tests d'intrusion...
- ❑ Contrôle / gestion des accès
- ❑ Mise à niveau des solutions technologiques
- ❑ Vérification des clauses de confidentialité
 - ✓ tiers (accès au réseau)
 - ✓ salarié

2 – discontinuité du service

- ❑ Réversibilité – transférabilité
- ❑ Solutions de contournement
- ❑ Sauvegardes et contrats de back-up
- ❑ Accès aux codes source

mais aussi.....

- ❑ Assurances
- ❑ Vérifications des contrats
 - ✓ Force majeure
 - ✓ Conséquences liées aux contrats

3 – perte des archives

- ❑ restituer l'information dans son intégrité
- ❑ dans le respect des prescriptions légales
 - 30 ans (contrats de travail, contrats de société...)
 - 10 ans (contrats commerciaux, factures,....)
 - 5 ans (documentation informatique relative aux traitements informatisés des données comptables...)

Actions :

- ✓ garanties de lisibilité des données et accessibilité
- ✓ garanties d'authenticité et d'intégrité des données
- ✓ pérennité des solutions techniques d'archivage
- ✓ identification et désignation des Données Sensibles
 - données et traitements assujettis aux contrôles fiscaux (ex : accès aux codes sources)

4 – atteinte à la vie privée des employés

□ Cybersurveillance = 3 principes

- ✓ Principe de proportionnalité
- ✓ Transparence de la cybersurveillance / salarié
- ✓ Transparence de la cybersurveillance / CE

□ Actions

- ✓ Charte sur l'utilisation des ressources informatiques
- ✓ Respect des principes en coordination avec RSSI-administrateur réseau

5 – non respect de la loi informatique et libertés

□ Définition

- ✓ toutes les données permettant d'identifier directement ou indirectement une personne physique
 - ex : adresse de courrier électronique, adresse IP...

□ Obligations

- ✓ déclaration préalable du traitement à la CNIL
- ✓ information de la personne concernée
 - droits d'accès, de rectification et d'opposition
- ✓ Respect du principe de loyauté et de finalité
- ✓ Sécurité du traitement

6 – non respect des règles de prospection commerciale

□ Principe de transparence :

- ✓ Identification des publicités
- ✓ Identification de l'émetteur du message ou du site
- ✓ Respect de la législation sur les offres promotionnelles

□ Principe de l'opt-in

- ✓ Sauf pour les produits ou services analogues fournis par la même personne physique ou morale et si le destinataire peut s'opposer sans frais
- ✓ Sauf lorsque le message est envoyé à des personnes physique : « au titre de la fonction qu'elles exercent dans l'organisme privé ou public qui leur a attribué cette adresse »

7 – non respect du CPI

☐ Risques

- ✓ Utilisation d'un logiciel sans licence ou non respect de la licence
- ✓ Site web/intranet contrefaisant des éléments protégés
- ✓ Bases de données

Actions :

- ✓ Veiller à la conclusion des licences et au respect de leur périmètre
- ✓ Vérifier les clauses de garantie d'éviction dans les contrats de logiciels
- ✓ Audits périodiques
- ✓ Tenir un registre des licences
- ✓ Actions de sensibilisation des utilisateurs

MERCI !