MEDEF

5. SECURITE DES TRAITEMENTS

Les organismes traitant des données personnelles doivent assurer la sécurité de ces traitements, en mettant en place des mesures (techniques et organisationnelles) appropriées aux risques identifiés pour sécuriser le traitement de ces données. **Cette obligation concerne non seulement les responsables de traitement, mais également les sous-traitants**.

1. Quels sont les types de précautions élémentaires à prendre ? *(cf. §3)*

Protéger les locaux	- Mettre en place des contrôles d'accès (vigiles, badges, biométrie…) - Installer un système de vidéosurveillance - Accompagner les visiteurs dans les locaux - Fermer à clé les locaux sensibles (contenant les dossiers RH par exemple ou encore les locaux des serveurs)
Sensibiliser les utilisateurs	- Sensibiliser le personnel - Rédiger une charte informatique - Prévoir une politique interne de sécurité (PSSI) en définissant par exemple des niveaux de classification des documents et mails
Sensibiliser les partenaires et prestataires	- Prévoir la signature d'engagements de confidentialité pour les prestataires - Prévoir une obligation de sécurité pour les sous-traitants
Prévoir un dispositif d'authentification	- Installer des mots de passe individuels sur les ordinateurs (session Windows par exemple) conformes aux règles définies par la CNIL - Installer des verrouillages automatiques de sessions en cas d'inactivité - Changer régulièrement les mots de passe
Gérer les accès et les habilitations	- Gérer les habilitations du personnel (limiter l'accès aux applications ou logiciels aux seuls utilisateurs qui en ont besoin dans le cadre de leurs missions, garder une trace des actions réalisées…) - Supprimer les habilitations des personnes quittant définitivement leurs fonctions - Mettre en place un système de journalisation (enregistrement des logs de connexion pour détecter des anomalies ou des incidents)
Sécuriser les postes de travail	- Mettre en place des antivirus, pare-feux… - Veiller à la mise à jour régulière des logiciels utilisés - Limiter et vérifier les supports mobiles (clés USB par exemple)
Sécuriser le réseau informatique	- Limiter les accès internet et les flux réseaux - Imposer un dispositif de sécurisation pour les accès à distance (VPN par exemple) - Veiller à la non-accessibilité des infrastructures depuis internet
Gérer la conservation des informations	- Mettre à disposition un espace de stockage - Effectuer des sauvegardes régulières des données - Prévoir des systèmes d'archivage

2. Comment sécuriser les traitements de données personnelles ?

Le responsable de traitement et le sous-traitant doivent mettre en place des mesures de sécurité adaptées aux risques (en fonction du degré de gravité et de probabilité de ces risques). Le RGPD préconise par exemples :

- La **pseudonymisation des données** (technique permettant de décorréler les données d'une personne et de ne pas réidentifier cette personne sans avoir recours à des informations supplémentaires conservées séparément)
- **Le chiffrement des données** (technique permettant de rendre la compréhension d'un document impossible à toute personne non autorisée)
- Des moyens permettant de **garantir la confidentialité, l'intégrité, la disponibilité et la résilience** des traitements de données personnelles
- Des moyens pour **rétablir la disponibilité des données** dans des délais appropriés en cas d'incident
- Une **procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures** de sécurité mises en place (audit de sécurité par exemple).

✓ Pour déterminer si une mesure est appropriée, il est tenu compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement.
✓ La mise en place de mesures de sécurité appropriées est prise en compte dans le calcul de la sanction de la CNIL et il est donc important à ce titre d'instaurer des principes basiques de sécurité.

3. Comment évaluer le niveau de sécurité approprié ?

Le responsable de traitement ou le sous-traitant doivent :

1. **Prendre en compte les risques** que représente le traitement de données personnelles, tels que :
   - La destruction, la perte, l'altération, la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière ;
   - L'accès non autorisé à de telles données, de manière accidentelle ou illicite.

2. Etablir un niveau de gravité

Niveaux de gravité	Descriptions	Exemples
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments qu'elles surmonteront sans difficulté.	- Perte de temps pour renouveler des démarches - Réception de courriers non sollicités - Simple contrariété (information non désirée, sentiment d'atteinte à la vie privée…)
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés.	- Diffamation - Paiement indu, frais supplémentaires - Refus d'accès à un service / prestation - Compte en ligne bloqué…
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.	- Détournement d'argent - Difficultés financières - Interdiction bancaire - Perte de données clientèle - Chantage…
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.	- Décès / Suicide - Péril financier / dettes importantes - Perte d'emploi - Sanction pénale…

CNIL – Echelle de gravité des risques pour les données personnelles

3. Mesurer le degré de probabilité des risques

4. Mettre en place des mesures de sécurité correctives pour réduire ce risque et le rendre acceptable *(cf. §1)*