

Toutes les entreprises sont concernées par

Le nouveau **Règlement Général de la Protection des Données**

(RGPD * ou GDPR)

Il harmonise et renforce la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données des citoyens européens. Il incite donc les sociétés à être vigilantes avec les informations qu'elles possèdent et qu'elles exploitent.

Sont concernées, toutes les entreprises (quelle que soit leur taille) qui possèdent des données sur les citoyens européens qu'elles soient situées en France ou dans le monde. Sa mise en vigueur est prévue **pour le 25 mai 2018.**

La sanction financière peut atteindre 4% du chiffre d'affaires mondial de l'exercice précédent.

REUSSIR SA MISE EN CONFORMITE EN QUELQUES ETAPES :

1] Sensibilisation :

Désignez un pilote (DPO*) suivant la nature des données traitées

2] Évaluation :

Cartographiez vos traitements de données personnelles, auditez vos solutions et

Identifiez des protections complémentaires si nécessaire

3] Stratégie :

Définissez votre politique de protection des données et vos actions à mener

4] Technologie :

Gérez les risques en choisissant vos options de gestion et de chiffrement

5] Preuve :

Documentez la conformité

L'anticipation est la clé de la réussite !

Vous ne pourrez pas y échapper.

Vous n'avez pas à le faire seul, nous sommes là pour vous accompagner.

Odette AMANN – Tél : 01.60.31.10.14 ou 06.08.27.61.76

odette.amann@ogi77.fr

**RGPD : Règlement Général de la Protection des Données / DPO : Data Privacy Officer*

PERTES ou FUITES D'INFORMATIONS

INTERNES

- **Clé USB** / support amovible
- **La messagerie**
- Usage de **we transfert / dropbox**
- Usage de mobile personnel à usage professionnel
- **Accès serveur** par les itinérants via leur ordinateur portable ou mobile
- **Accès à des sites non professionnels** : (téléchargement de *Malwares / logiciels espions*)
- Consultation de la **messagerie personnelle via l'ouverture d'une pièce jointe (ransomware, etc...)**
- **Usage du wifi de l'entreprise** pour le mobile personnel
- **Sauvegardes non-effectuées** correctement ou non envoyées vers le serveur

EXTERNES

- **Mot de passe faible** : réseau, wifi, mail...
- **Windows serveur osbolète (<= 2003)**
- Accès au serveur via du **matériel d'un itinérant volé et mal sécurisé**
- **Points d'accès** à l'entreprise **non sécurisés** (ex : accès via http ou TSE par ports standards 3389)
- **Vidéosurveillance** reliée au réseau informatique

SOLUTIONS APPORTEES PAR OGI

- **Sécuriser les ports routeurs**
- **Bloquer les plateformes** de téléchargement non-autorisées, et choisir **une plateforme sécurisée** pour l'ensemble des transferts de l'entreprise (*I Extranet et Postfile de Oodrive*...)
- **Coupler les sauvegardes internes avec celles** en Data Center (*AdBackup de Oodrive*)
- **Cryptage des disques durs des portables** pour protection des informations confidentielles
- **Protection de vos accès réseaux** externes avec un **VPN**, un **certificat SSL** et une **double authentification**
- Restreindre les droits **du profil utilisateur** pour éviter les installations de logiciels non-autorisés
- Filtrage de **navigation internet**
- **Contrôle anti-virus** des fichiers
- **Filtrage des messageries** : anti-spam et anti-virus en amont
- **Authentification des mobiles professionnels** sur le wifi pour exclure les accès aux mobiles non autorisés qui peuvent aussi alourdir la bande passante