

Check-list RGPD en 12 étapes pour PME

Une feuille de route claire et actionnable pour structurer votre conformité RGPD.

1. Identifier les données personnelles collectées

Inventorier les données RH, clients, prospects, fournisseurs.

Objectif : savoir *ce que vous traitez* avant de décider *comment le protéger*.

2. Cartographier les traitements

Lister les activités impliquant des données : recrutement, facturation, CRM, SAV, emailing, site web...

3. Compléter le Registre des Traitements

Document obligatoire, base de toute mise en conformité.

4. Vérifier la licéité des traitements

Associer chaque traitement à une base légale : contrat, consentement, obligation légale...

5. Mettre à jour les mentions d'information

Site internet, formulaires, devis, politique de confidentialité, clauses contractuelles.

6. Revoir les contrats fournisseurs & sous-traitants

Ajout de clauses RGPD.

Vérification des outils SaaS utilisés.

7. Encadrer les transferts hors UE

Vérifier si vos outils (CRM, email, cloud) transfèrent des données.

8. Gérer les droits des personnes

Mettre en place un processus : accès, rectification, opposition, suppression.

9. Durées de conservation

Fixer des durées logiques : RH, clients, prospects, caméras, cookies...

10. Sécuriser les systèmes

Contrôle des accès, mots de passe, MFA, sauvegardes, gestion des habilitations.

11. Préparer la gestion des violations

Document obligatoire : procédure + registre des incidents.

12. Sensibiliser les équipes

Formation annuelle recommandée pour RH, commerce, informatique, direction.