

CHECKLIST DE CONFORMITÉ RGPD

Vérifiez et maintenez votre conformité RGPD point par point.

Rappel : **Le registre des activités de traitement est OBLIGATOIRE** (art. 30 RGPD). En cas de contrôle, son absence expose à une amende jusqu'à 20 millions € ou 4 % du chiffre d'affaires annuel.

Cette check-list vous aide à vérifier les points essentiels.

Cochez les cases correspondant à votre situation.

1. DONNÉES PERSONNELLES ET REGISTRE - **Priorité maximale**

- ☐ J'ai une politique de confidentialité (même si je n'ai pas de site internet)
- ☐ J'ai créé et je tiens à jour un registre des activités de traitement (RGPD).
- ☐ J'ai listé toutes les catégories de données que je collecte.
- ☐ Je limite la collecte des données au strict nécessaire (minimisation).
- ☐ J'ai fixé des durées de conservation pour chaque catégorie de données.
- ☐ J'applique une politique de destruction sécurisée à l'échéance.

2. RELATION CLIENT ET CONSENTEMENTS - **Priorité maximale**

- ☐ Je recueille un consentement écrit explicite de chaque client pour la collecte des données de santé et autres données sensibles (parcours personnel, état émotionnel ...)(formulaire RGPD).
- ☐ Je conserve la preuve des consentements (formulaires signés, cases cochées ...).
- ☐ Mes clients sont informés de leurs droits RGPD (accès, rectification, effacement, opposition) dans au moins un des documents que je leur remets.

3. OUTILS NUMÉRIQUES ET SOUS-TRAITANTS - **Priorité maximale**

- ☐ J'ai signé un DPA (Data Processing Agreement) avec chaque sous-traitant (hébergeur, logiciel de gestion, plateforme de réservation, outil de visio, comptable, etc.).
- ☐ Je privilégie les outils hébergés dans l'Union européenne (France de préférence).
- ☐ Je vérifie la politique de confidentialité de chaque nouvel outil avant de l'utiliser.

- ☐ Je limite les accès à mes comptes professionnels (pas de partage des mots de passe).

4. GESTION ADMINISTRATIVE ET COMPTABLE - Priorité maximale

- ☐ Je conserve les documents comptables (factures) pendant 10 ans (obligation légale).
- ☐ Je sécurise mes factures et documents financiers (accès restreint, chiffrement).
- ☐ J'utilise des solutions de paiement conformes (Stripe, PayPal, etc. - DPA signé).

5. STOCKAGE ET SÉCURITÉ DES DONNÉES - Priorité importante

- ☐ J'utilise des mots de passe robustes (12+ caractères, chiffres, symboles, majuscules).
- ☐ J'utilise un gestionnaire de mots de passe (Dashlane, Bitwarden, etc.).
- ☐ J'ai activé la double authentification (2FA) sur tous mes outils professionnels.
- ☐ Je chiffre mes appareils (ordinateur, smartphone, tablette).
- ☐ Je fais des sauvegardes régulières et sécurisées (chiffrées, hors ligne).
- ☐ Je verrouille mes armoires et dossiers papier (clé séparée).
- ☐ Je supprime les données dès que la durée de conservation est expirée.

6. SÉANCES À DISTANCE (VISIOCONFÉRENCE) - Priorité importante

- ☐ J'utilise des outils de visioconférence conformes RGPD (hébergement UE ou DPA signé).
- ☐ Je sécurise mes sessions avec un mot de passe et une salle d'attente.
- ☐ J'informe mes clients de l'outil de visioconférence utilisé.
- ☐ Je n'enregistre jamais les séances sans consentement exprès écrit du client.

7. COMMUNICATION ET ÉCHANGES - Recommandé

- ☐ J'utilise une messagerie sécurisée pour les échanges contenant des données sensibles.
- ☐ Je ne discute pas de cas clients dans des lieux publics.
- ☐ Avant de publier sur les réseaux sociaux, je vérifie que le contenu ne comporte aucune allégation thérapeutique / médicale, ni garantie de résultat (vocabulaire conforme, pas de données clients).

8. SÉANCES À DOMICILE ET DÉPLACEMENTS - Recommandée

- ☐ Je transporte les dossiers clients dans une sacoche ou enveloppe sécurisée (pas à vue).
- ☐ Je ne laisse pas de documents ou d'ordinateur dans mon véhicule.
- ☐ J'efface mon historique de navigation après les déplacements (si ordinateur partagé).
- ☐ J'utilise un cahier ou un bloc dédié (pas de feuilles volantes non archivées).

9. BONNES PRATIQUES SUPPLÉMENTAIRES - Facultatif

- ☐ J'utilise un gestionnaire de mots de passe sécurisé.
- ☐ Je nettoie régulièrement mes emails et fichiers (suppression des données inutiles).
- ☐ Je fais des « tests de sécurité » occasionnels (antivirus, mise à jour, double authentification).

PLAN D'ACTION PRIORITAIRE

Priorité	Point à corriger	Action concrète	Délai cible	Fait
Max	☐			
Max	☐			
Importante	☐			
Importante	☐			

Date de la vérification : _____

Prochaine révision prévue : _____ (dans 6 mois recommandé)