

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

🔴 **DOCUMENT MIS A JOUR : 12-03-2025**

1. POLITIQUE DE CONFIDENTIALITÉ

La politique de confidentialité est le document principal qui informe les utilisateurs sur les données personnelles collectées, leur traitement, et leurs droits. Elle doit inclure :

- **Les coordonnées du responsable du traitement** : M. Guillaume Friboulet (PDG de Normandie Taxis Academy).
- **Finalités du traitement des données.**
- **Base légale des traitements** (exécution d'un contrat, obligation légale, consentement, etc.).
- **Les droits des utilisateurs** (accès, rectification, opposition, effacement, portabilité, etc.).
- **Durée de conservation des données.**
- **Mesures de sécurité mises en place.**
- **Utilisation des cookies et gestion des consentements.**
- **Utilisation de Google Analytics** : Détailler que les données sont anonymisées, que les utilisateurs peuvent refuser ce traitement, et mentionner les garanties offertes pour les transferts hors UE.
- **Mise à jour régulière** : Indiquer que cette politique est révisée au moins une fois par an.

2. REGISTRE DES ACTIVITÉS DE TRAITEMENT

Un registre détaillant toutes les activités de traitement est obligatoire. Celui-ci inclut :

- **Catégories de données collectées** (nom, prénom, email, téléphone, etc.).
- **Finalités de chaque traitement** (inscription, suivi administratif, envoi d'informations, etc.).
- **Base légale de chaque traitement.**
- **Durée de conservation pour chaque catégorie de données.**
- **Mesures techniques et organisationnelles pour sécuriser les données.**
- **Exemple** : Pour les inscriptions, collecte des noms, emails et téléphones dans le cadre de l'exécution du contrat de formation, conservés pendant 3 ans après la fin de la formation.
- **Processus de mise à jour** : Audit annuel pour garantir la mise à jour des données et des traitements.

3. CHARTE DE SÉCURITÉ

La charte de sécurité détaille les mesures mises en œuvre pour protéger les données personnelles :

- **Authentification forte** (mots de passe complexes, double authentification).
- **Chiffrement des données sensibles.**
- **Sauvegardes régulières.**

- **Accès restreint aux données.**
- **Audit de sécurité interne** : Réalisé annuellement pour vérifier l'efficacité des mesures mises en œuvre.
- **Formation continue des administrateurs** pour identifier et corriger les failles potentielles.

4. ENGAGEMENTS INTERNES

Les engagements pris par les collaborateurs internes doivent être formalisés par des clauses spécifiques de confidentialité et de protection des données dans leurs contrats de travail. Ces engagements incluent :

- La confidentialité des données traitées.
- La sensibilisation aux risques de violation.
- L'obligation de signaler tout incident de sécurité.
- **Archivage** : Les preuves des engagements sont conservées en cas d'audit RGPD.

5. PROCÉDURE DE GESTION DES VIOLATIONS DE DONNÉES

Une procédure claire doit être mise en place pour identifier, signaler, et gérer les violations de données personnelles :

- **Détection** : Surveillance des systèmes pour identifier les failles.
- **Notification** : Obligation de notifier la CNIL dans les 72 heures en cas de risque élevé.
- **Documentation** : Tenue d'un registre des violations.
- **Correction** : Mise en œuvre rapide des mesures correctives.
- **Exemple** : En cas d'accès non autorisé aux données, identification immédiate de la source, blocage des accès compromis, notification aux utilisateurs concernés, et rapport à la CNIL.

6. FORMATION ET SENSIBILISATION

Des formations régulières doivent être organisées pour les collaborateurs afin de :

- Les sensibiliser aux enjeux de la protection des données.
- Leur apprendre à identifier les risques liés aux violations.
- Les informer des bonnes pratiques.
- **Fréquence** : Sessions biannuelles et mises à jour lors de tout changement réglementaire majeur.
- **Trace documentaire** : Attestations de présence et programmes archivés pour chaque session de formation.

7. GESTION DES DROITS DES UTILISATEURS

Une procédure doit être mise en place pour répondre efficacement aux demandes d'exercice de droits (accès, rectification, suppression, portabilité, etc.) :

- **Point de contact dédié** : normandietaxisacademy@gmail.com.
- **Délai de réponse** : Maximum d'un mois (ou deux mois en cas de complexité).
- **Documentation** : Conservation des traces des demandes et des réponses apportées.

- **Modèle de suivi** : Un registre interne mentionnant la date de la demande, la nature de la demande, et la date de réponse.
- **Gestion des demandes abusives** : Mention explicite que les demandes manifestement infondées ou excessives peuvent être rejetées ou facturées.

8. POLITIQUE DE CONSERVATION DES DONNÉES

Un calendrier précis doit être établi pour détruire ou anonymiser les données une fois leur durée de conservation écoulée.

Exemple :

- Données d'inscription : Conservation pendant la durée de la formation + 3 ans.
- Données techniques (cookies) : Conservation pendant 1 an.
- **Processus d'archivage** : Vérification trimestrielle des données obsolètes et suppression selon les normes sécurisées.

9. POLITIQUE DE COOKIES

Les cookies utilisés sur le site doivent être documentés dans une politique dédiée, mentionnant :

- Leur finalité (techniques, analytiques, marketing).
- La durée de conservation des cookies.
- Les moyens pour les utilisateurs de gérer leurs préférences.
- **Outils tiers** : Par exemple, Google Analytics (suivi statistique), avec les données anonymisées et les options de refus claires via le bandeau de consentement.
- **Mise à jour dynamique** : Les utilisateurs sont informés des changements apportés à la politique via une bannière ou un email dédié.

10. AUDITS RGPD

Des audits internes réguliers permettent de vérifier la conformité continue avec la réglementation.

Ces audits incluent :

- La revue du registre des activités de traitement.
- La vérification des mesures de sécurité.
- La mise à jour des politiques et procédures en fonction des évolutions légales.
- La vérification des outils et services utilisés, en s'assurant qu'ils respectent le RGPD.
- Fréquence : Un audit annuel minimum.
- Rapport d'audit : Chaque audit donne lieu à un rapport documentant les observations et les recommandations.

11. DOCUMENTATION COMPLÈTE

Tous les documents doivent être centralisés et accessibles en cas de contrôle ou d'audit externe :

- Politique de confidentialité.
- Registre des activités de traitement.
- Charte de sécurité.
- Engagements internes.
- Documentation sur les cookies.
- Procédure de gestion des violations.
- Documentation sur les transferts hors UE.
- Historique des mises à jour : Liste datée des révisions de chaque document.

12. TRANSFERTS HORS UE

Si des données sont transférées en dehors de l'UE, les garanties suivantes doivent être mentionnées :

- Utilisation des **Clauses Contractuelles Types (CCT)**.
- Vérification de la conformité des prestataires aux standards européens.
- Notification claire dans la politique de confidentialité.
- Évaluation périodique des transferts : Examen annuel des transferts pour garantir leur conformité.

Pour toute question relative à la protection des données, contactez : **normandietaxisacademy@gmail.com**