RGPD - Plan de mise en conformité (draft)

Désignation des responsables des données et des traitements

- Le Responsable du traitement : responsable des outils informatiques.
- Délégué à la protection des données : ***Facultatif pour notre cas.***

Liste de contrôle

Etapes principales		**Conformité : oui/non**
Analyser la situation — Réalisation d'un audit sur les données	• Mon organisation sait quelles données à caractère personnel de résidents de l'UE elle héberge et traite actuellement (et les a documentées). • Elle a une connaissance précise des méthodes utilisées pour collecter toutes ces données. • Elle sait où ces données sont conservées. • Elle est au courant de tous les tiers qui traitent de telles données pour son compte.	
Planifier — Mise au point d'un plan de correction	• Mon organisation a créé et communiqué une politique relative à la protection et au traitement des données personnelles. • Elle a établi un plan de détection, de réponse aux incidents et de signalement pour les violations de données à caractère personnel de citoyens de l'UE.	
Protéger — Mise en oeuvre des technologies et processus adéquats	• Mon organisation a désigné un délégué à la protection des données. • Son comité d'administration (comité directeur) est dûment informés du programme relatif au RGPD et impliqués dans celui-ci.	

	• Mon organisation a mis en place un programme de sensibilisation des utilisateurs à la protection des données. • Elle collecte les données à caractère personnel sur consentement de la personne concernée. • Elle a mis en oeuvre des solutions de sécurité avancées pour prévenir les violations de données.	
Optimiser — Évaluations régulières pour contrôler l'efficacité des mesures mises en oeuvre	• Mon organisation dispose d'un processus permettant de tester l'efficacité des mesures de protection des données (mesures mises en place en interne et par tous les tiers qui traitent des données). • Elle analyse tous les nouveaux processus et systèmes traitant des données à caractère personnel de résidents de l'UE afin d'évaluer l'impact de la protection des données.	

Etapes complémentaires	Conformité : oui/non	Commentaires
Identification et de recensement des données à caractère personnel qui sont stockées et/ou traitées		
Pertinence de conserver et/ou traiter ces données et de la pertinence de la finalité des traitements		
Sécurité attachée à l'intégrité, à la confidentialité et à l'accès des données réalisée		
Vérification que ces données ne sont pas des données sensibles (race, religion, …) et que ces personnes concernées sont informées de la détention et/ou du traitement de ces données et qu'elles ont donné leur accord		
Analyse à l'aide de fiches les traitements et les données		
Analyse de risque et, si le risque est élevé, une analyse d'impact sur la vie privée (voir outil CNIL) https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil		
Signalement aux personnes concernées et, dans les 72h à la CNIL toute disparition ou violation concernant ces données		
Informer les sous-traitants informatiques de leurs responsabilités en matière de traitement de données personnelles et mise en place d'avenants aux contrats		
Informer au fil de l'eau des tiers s'il y a échange de données personnelles, mention spécifique à		

insérer dans les modèles de contrat et mise en place éventuelle d'avenants aux contrats		
Définir les modalités d'accès aux informations par les personnes concernées aux fins d'information, de rectification, d'effacement, de limitation de traitement ou de portabilité.		
Organiser la Gouvernance, responsable et/ou DPO à désigner, code de conduite à rédiger.		
Documentation à conserver de toutes ces étapes, dossier numérique RGPD à organiser, Registre et fiches registre à tenir à jour.		
Mettre à niveau si besoin la sécurité informatique en relation avec les données :		
Contrôler l'accès aux données de façon adaptée, accès en local ou à distance		
Imposer l'authentification et des mots de passe sécurisés		
Stocker et communiquer les informations sensibles de manière sécurisée (chiffrement)		
Appliquer une sécurité rigoureuse sur les nouveaux traitements		
S'assurer que les prestataires de services mettent en place des mesures de sécurité informatique		
Avoir des procédures de maintien de la sécurité et de correction des vulnérabilités.		