ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE MON ORGANISME

Avez-vous pensé à... ?

FICHES		MESURES	
1	Piloter la sécurité des données	Faire de la sécurité un enjeu partagé et porté par l'équipe dirigeante	☐
		Évaluer régulièrement l'efficacité des mesures de sécurité mises en œuvre et adopter une démarche d'amélioration continue	☐
2	Définir un cadre pour les utilisateurs	Rédiger une charte informatique comprenant les modalités d'utilisation des systèmes informatiques, les règles de sécurité et les moyens d'administration en place	☐
		Donner une force contraignante à la charte et y rappeler les sanctions encourues en cas de non-respect	☐
3	Impliquer et former les utilisateurs	Sensibiliser les personnes manipulant les données	☐
		Adapter le contenu des sensibilisations à la population ciblée et à leurs tâches	☐
4	Authentifier les utilisateurs	Octroyer un identifiant (« *login* ») unique à chaque utilisateur	☐
		Adopter une politique de mot de passe conforme aux recommandations de la CNIL	☐
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	☐
5	Gérer les habilitations	Définir des profils d'habilitation	☐
		Supprimer les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
6	Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session	☐
		Installer et configurer un pare-feu (« *firewall* » en anglais) logiciel	☐
		Utiliser des antivirus régulièrement mis à jour	☐
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	☐
7	Sécuriser l'informatique mobile	Sensibiliser les utilisateurs aux risques spécifiques du nomadisme	☐
		Prévoir des moyens de chiffrement des équipements mobiles	☐
		Exiger un secret pour le déverrouillage des smartphones	☐
8	Protéger le réseau informatique	Limiter les flux réseau au strict nécessaire	☐
		Sécuriser les réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3	☐
		Sécuriser les accès distants des appareils informatiques nomades par VPN	☐
		Cloisonner le réseau, entre autres en mettant en place une DMZ (zone démilitarisée)	☐
9	Sécuriser les serveurs	Désinstaller ou désactiver les services et interfaces inutiles	☐
		Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installer sans délai les mises à jour critiques après les avoir testées le cas échéant	☐

FICHES		MESURES	
10	Sécuriser les sites web	Sécuriser les flux d'échange des données	☐
		Vérifier qu'aucun secret ou donnée personnelle ne passe par les URL	☐
		Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu	☐
11	Encadrer les développements informatiques	Prendre en compte la protection des données personnelles dès la conception	☐
		Proposer des paramètres respectueux de la vie privée par défaut	☐
		Réaliser des tests complets avant la mise à disposition ou la mise à jour d'un produit	☐
		Utiliser des données fictives ou anonymisées pour le développement et les tests	☐
12	Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées	☐
		Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
13	Sécuriser les échanges avec l'extérieur	Chiffrer les données avant leur envoi	☐
		S'assurer qu'il s'agit du bon destinataire	☐
		Transmettre le secret lors d'un envoi distinct et via un canal différent	☐
14	Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants	☐
		Prévoir les conditions de restitution et de destruction des données	☐
		S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, visites)	☐
15	Encadrer la maintenance et la fin de vie des matériels et des logiciels	Enregistrer les interventions de maintenance dans une main courante	☐
		Encadrer les interventions de tiers par un responsable de l'organisme	☐
		Effacer les données de tout matériel avant sa mise au rebut	☐
16	Tracer les opérations	Prévoir un système de journalisation	☐
		Informer les utilisateurs de la mise en place du système de journalisation	☐
		Protéger les équipements de journalisation et les informations journalisées	☐
		Analyser régulièrement les traces pour détecter la survenue d'un incident	☐
17	Sauvegarder	Effectuer des sauvegardes régulières	☐
		Protéger les sauvegardes, autant pendant leur stockage que leur convoyage	☐
		Tester régulièrement la restauration des sauvegardes et leur intégrité	☐

FICHES		MESURES	
18	Prévoir la continuité et la reprise d'activité	Prévoir un plan de continuité et de reprise d'activité	☐
		Effectuer des exercices régulièrement	☐
19	Gérer les incidents et les violations	Traiter les alertes remontées par le système de journalisation	☐
		Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles	☐
20	Analyse de risques	Mener une analyse de risques, même minimale, sur les traitements de données envisagés	☐
		Suivre au cours du temps l'avancement du plan d'action décidé à l'issue de l'analyse de risques	☐
		Revoir régulièrement l'analyse de risques	☐
21	Chiffrement, hachage, signature	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	☐
		Conserver les secrets et les clés cryptographiques de manière sécurisée	☐
22	*Cloud* : Informatique en nuage	Inclure les services *cloud* dans l'analyse de risques	☐
		Évaluer la sécurité mise en place par le fournisseur	☐
		Veiller à la répartition des responsabilités de sécurité dans le contrat	☐
		Assurer le même niveau de sécurité dans le *cloud* que sur site	☐
23	Applications mobiles : Conception et développement	Prendre en compte les spécificités de l'environnement mobile pour réduire les données personnelles collectées et limiter les permissions demandées	☐
		Encapsuler les communications dans un canal TLS	☐
		Utiliser les suites cryptographiques du système d'exploitation et les protections matérielles des secrets	☐
24	Intelligence artificielle : Conception et apprentissage	Adopter les bonnes pratiques de sécurité applicables au développement informatique	☐
		Veiller à la qualité et l'intégrité des données utilisées pour l'apprentissage et l'inférence	☐
		Documenter le fonctionnement et les limitations du système	☐
25	API : Interfaces de programmation applicative	Organiser et documenter la sécurité des accès aux API et aux données	☐
		Limiter le partage des données uniquement aux personnes et aux finalités prévues	☐