Évaluer le niveau de sécurité des données personnelles de votre organisme

Avez-vous pensé à ... ?

Fiches		Mesures	
1	**Sensibiliser les utilisateurs**	Informer et sensibiliser les personnes manipulant les données	□
		Rédiger une charte informatique et lui donner une force contraignante	□
2	**Authentifier les utilisateurs**	Définir un identifiant (« login ») unique pour chaque utilisateur	□
		Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL	□
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	□
		Limiter le nombre de tentatives d'accès à un compte	□
3	**Gérer les habilitations**	Définir des profils d'habilitation	□
		Supprimer les permissions d'accès obsolètes	□
		Réaliser une revue annuelle des habilitations	□
4	**Tracer les opérations et gérer les incidents**	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	□
		Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles	□
5	**Sécuriser les postes de travail**	Prévoir une procédure de verrouillage automatique de session	□
		Utiliser des antivirus régulièrement mis à jour	□
		Installer un pare-feu (« firewall ») logiciel	□
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	□
6	**Sécuriser l'informatique mobile**	Prévoir des moyens de chiffrement des équipements mobiles	□
		Faire des sauvegardes ou des synchronisations régulières des données	□
		Exiger un secret pour le déverrouillage des smartphones	□
7	**Protéger le reseau informatique interne**	Limiter les flux réseau au strict nécessaire	□
		Sécuriser les accès distants des appareils informatiques nomades par VPN	□
		Sécuriser ses réseaux Wi-Fi, notamment en mettant en oeuvre le protocole WPA3	□
8	**Sécuriser les serveurs**	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	□
		Installer sans délai les mises à jour critiques	□
		Assurer une disponibilité des données	□
9	**Sécuriser les sites web**	Utiliser le protocole TLS et vérifier sa mise en oeuvre	□
		Vérifier qu'aucun mot de passe ou donnée personnelle ne passe par les URL	□
		Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu	□
		Mettre un bandeau de consentement pour les cookies non nécessaires au service	□
10	**Sauvegarder et prévoir la continuité d'activité**	Effectuer des sauvegardes régulières	□
		Stocker les supports de sauvegarde dans un endroit sûr	□
		Protéger les sauvegardes, notamment durant leur convoyage	□
		Prévoir et tester régulièrement la continuité d'activité	□

11	**Archiver de manière sécurisée**	Mettre en oeuvre des modalités d'accès spécifiques aux données archivées	□
		Détruire les archives obsolètes de manière sécurisée	□
12	**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	□
		Éviter les zones de commentaires ou les encadrer strictement	□
		Utiliser des données fictives ou anonymisées pour le développement et les tests	□
13	**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	□
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	**Sécuriser les échanges avec d'autres organismes**	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	□
16	**Protéger les locaux**	Restreindre les accès aux locaux au moyen de portes verrouillées	□
		Installer des alarmes anti-intrusion et les vérifier périodiquement	□
17	**Chiffrer, hacher ou signer**	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	□
		Conserver les secrets et les clés cryptographiques de manière sécurisée	□