Bonnes pratiques sécurité données RGPD		
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 à chaque utilisateur
		Adopter une politique de mot de passe utilisateur conforme aux recommandations CNIL
		Obliger l'utilisateur à changer son mot de passe après réinitialisation
		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 accès 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 pour les notifications de violation de données à caractère personnel
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
6	Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
		Faire des sauvegardes ou synchronisations régulières des données
		Exiger un code secret pour le déverrouillage des smartphones
7	Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
		Sécuriser les accès distants des appareils informatiques nomades par VPN
		Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
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
9	Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
		Vérifier qu'aucun mot de passe ou identifiant ne passe dans 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
		Prévoir et tester régulièrement la continuité d'activité
11	Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
		Détruire les archives obsolètes de manière sécurisée
12	Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
		Encadrer par un responsable de l'organisme les interventions par des tiers
		Effacer les données de tout matériel avant sa mise au rebut
13	Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
		Prévoir les conditions de restitution et de destruction des données
		S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
14	Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
		S'assurer qu'il s'agit du bon destinataire
		Transmettre le code secret lors d'un envoi distinct et via un canal différent
15	Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
		Installer des alarmes anti-intrusion et vérifiez-les périodiquement
16	Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
		Tester sur des données fictives ou anonymisées
17	Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
		Conserver les codes secrets et les clés cryptographiques de manière sécurisée

Adaptation d'une source officielle de la CNIL sur la sécurisation des organisations

www.rgpdchr.fr

dcampagne@rgpdchr.fr

@rgpdchr.fr