Check-List mise en conformité du cabinet au RGPD

N°	Action	Commentaire	Fait	A faire
1.	Recenser les fichiers, dossiers, répertoires, logiciels, dossiers ou archives papier contenant de la donnée à caractère personnel	La donnée peut concerner des clients, contacts prospects, salariés, stagiaires, collaborateurs libéraux, fournisseurs, adversaires, experts, magistrats…		
2.	Désigner un référent RGPD au cabinet ou un DPO volontaire ou externe	Se référer au guide du CNB ou de la CNIL pour les PME		
3.	En regroupant les fichiers par finalités (gestion client, facturation-recouvrement, recrutement…), commencer à formaliser un registre des traitements en tant que responsable des traitements	Un modèle-type de registre est disponible sur l'Encyclopédie des avocats. Ce document est obligatoire (article 30 du RGPD).		
4.	Supprimer les fichiers et données inutiles ou allant au-delà de la durée de conservation fixée	Cette opération est aussi appelée « purge » des données. Se référer au référentiel de durées de conservation des données et documents disponible sur l'Encyclopédie des avocats.		
5.	Dresser la liste de vos « sous-traitants » au sens du RGPD (prestataires informatiques, hébergeur, agence web, événementielle ou de communication…)	Consigner cette liste à l'aide du modèle de registre des sous-traitants disponible sur l'Encyclopédie des avocats.		
6.	Conclure avec chaque sous-traitant une clause sous-traitance (« data processing agreement ») conforme à l'article 28 du RGPD	Vérifier que votre contrat avec le sous-traitant contient une clause ou une annexe répondant aux exigences de l'article 28 du RGPD. A défaut utiliser le modèle de clause de la CNIL ou celui disponible sur l'Encyclopédie des avocats.		
7.	Penser à tenir une documentation (tableau) recensant les incidents de sécurité (violation de données)	Une violation de données peut être simplement une perte de clé USB ou encore la perte de votre PC. Un modèle de documentation (sous la forme d'un registre) est disponible sur l'Encyclopédie des avocats. Cette documentation est obligatoire (article 33 du RGPD).		
8.	Registre des demandes d'exercice de droits adressées au cabinet	Un modèle de registre est disponible sur l'Encyclopédie des avocats.		
9.	Formaliser une politique des personnes habilitées à accéder au système d'information du cabinet	La gestion des accès au système d'information doit permettre de minimiser les accès et ainsi les risques. Elle est fondée sur le principe du « besoin d'en connaître ». Tout le monde n'a pas besoin d'avoir accès à tous les fichiers.		
10.	Signer une clause de confidentialité avec tous les salariés, collaborateurs, intervenants extérieurs	La clause doit bien viser les données nominatives comme étant confidentielles		
11.	Adopter une charte informatique au sein du cabinet	Cette charte d'utilisation des ressources informatiques vise à informer les membres du cabinet sur les bonnes		

		pratiques, notamment en ce qui concerne les usages de BYOD : Bring Your Own Device. Un modèle de charte est disponible sur l'Encyclopédie des avocats.		
12.	Ajouter à sa convention d'honoraires une clause données personnelle conforme aux recommandations de la CNIL, du CNB et du Barreau de Paris	Un modèle de convention à jour est disponible sur l'Encyclopédie des avocats.		
13.	Ajouter au contrat de collaboration libérale une clause donnée personnelle	Un modèle de contrat à jour est disponible sur l'Encyclopédie des avocats.		
14.	En cas de vidéosurveillance au cabinet, la limiter à la zone d'accueil du public à l'entrée du cabinet, la mentionner au registre, ne pas conserver les données d'enregistrement plus d'un mois et afficher à l'accueil le recours la vidéosurveillance	A défaut, encadrer les flux transfrontières avec les outils disponibles (clauses contractuelles types de la commission européenne) et en informer les personnes concernées. Se référer au guide RGPD du CNB pour plus de précisions.		
15.	Privilégier des services informatiques et numériques notamment *cloud* dont les données sont localisées au sein de l'Union européenne et de l'EEE.	Dès lors qu'il s'agit d'un opérateur *cloud* dont la maison mère est située hors UE, et même si celui-ci garantit l'hébergement des données en UE, il convient de documenter le transfert de données hors UE résultant de l'utilisation de ce service (documenter ces flux en reprenant la politique de confidentialité du fournisseur *cloud*) ou bien s'adresser à un autre opérateur européen.		
16.	En cas de transfert de données à caractère personnel dans des pays tiers non adéquats (article 45 du RGPD), vérifier que le transfert est protégé par des garanties appropriées de protection (article 46 du RGPD : clauses contractuelles types de la Commission européenne, règles d'entreprise contraignantes…) et que celles-ci sont assorties de mesures supplémentaires de protection pour des pays où la législation nationale met à mal les garanties contenues dans l'outil d'encadrement du transfert en diminuant ou écartant l'application de ces garanties.	Mener un Transfert Impact Assessment pour vérifier ces points. Le groupe « Meta » (Facebook, Instagram…) a été condamné à verser 1,2 milliard d'euros car les clauses contractuelles types sur lesquelles il se fonde pour transférer des données vers les Etats-Unis n'est pas assortie de mesures supplémentaires de protection (techniques et organisationnelles).		
17.	Revoir la politique de confidentialité de son site web conformément aux recommandations de la CNIL et du CNB	Ne pas omettre les mentions d'information nécessaires si vous utilisez un formulaire de contact et les mentions des droits des personnes concernées. Un modèle est disponible sur l'Encyclopédie des avocats dans une annexe au guide RGPD intitulée « Modèles de mentions d'information RGPD).		
18.	Mettre un bandeau cookies sur son site internet conformément aux recommandations de la CNIL	Consulter les recommandations de la CNIL en la matière et se référer au guide RGPD du CNB pour plus de précisions.		

19.	Eviter d'utiliser les outils de type cookies traceurs avec transfert de données à l'international (de type Google Analytics, risque de mise en demeure par la CNIL)	Utiliser les alternatives proposées par la CNIL.		
20.	S'assurer de connaître et maitriser les bases de l'organisation du Système d'Information du cabinet	Savoir notamment si vous utilisez un serveur physique, un serveur dématérialisé Cloud.		
21.	Utiliser un VPN et Installer un pare-feu (firewall)			
22.	Installer et mettre à jour régulièrement son anti-virus & mettre à jour ses systèmes d'exploitation			
23.	Ne pas utiliser des logiciels de transferts grand public non sécurisés lorsque vous transférer des données.			
24.	Choisir des mots de passe conformes aux recommandations de la CNIL & changer de mot de passe à intervalle régulier	Mots de passe robustes basés sur l'entropie. Pour tester le niveau d'entropie de son mot de passe, la CNIL propose cet outil : https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe.		
25.	Centraliser les données du cabinet en un point en réseau et non en local sur les postes (facilité de partage, de sauvegarde, de sécurisation, de gestion des accès, de contrôle de la sécurité pour déceler les anomalie éventuelles	Avoir une politique de gestion des droits d'accès. Cloisonner données personnelles / données privées : le plus possible, créer des profils séparés : ne voit les données que qui en a besoin		
26.	Prévoir une procédure en cas de perte/vol des PC portables	Chiffrer le disque dur de chaque PC portable utilisé au cabinet		
27.	Mettre en place une solution de continuité de l'activité. Assurer une formation minimale sur les risques et les bonnes pratiques informatiques pour chaque membre du cabinet	Si vous vous reposez exclusivement sur votre hébergeur pour la sauvegarde, vérifier qu'au moins une copie de sauvegarde est faite hors site. En cas de cyber-attaque, la meilleure première action est d'éteindre le PC et le déconnecter d'internet		