

Exemple de check-list « informatique et libertés »

1	Le projet informatique constitue-t-il bien un traitement de données à caractère personnel soumis au RGPD ? Suis-je responsable de traitement ou sous-traitant au sens du RGPD ? Le RGPD s'applique-t-il bien au traitement (loi applicable) ? Puis-je bénéficier du dispositif de « guichet unique » (traitements paneuropéens) ?
2	Une politique de documentation de la conformité est-elle mise en œuvre ? Si oui, dans quelles conditions exactes (registre des traitements, <i>privacy by design</i> , procédures, clausiers, réalisation d'études d'impact, audit, formation des personnels, etc.) ? En particulier : – Dois-je tenir à jour un registre des activités de traitement ? – Dois-je désigner un délégué à la protection des données (DPD) ? – Dois-je rédiger une étude d'impact (PIA) ?
3	La collecte des données du traitement est-elle licite, loyale et transparente ?
4	Le principe de proportionnalité et de minimisation des données est-il respecté (concernant notamment la finalité du traitement et les catégories de données collectées) ?
5	Une durée de conservation des données a-t-elle été définie ? Des modalités d'archivage des données ont-elles été définies ?
6	Une politique de sécurité et de confidentialité des données est-elle définie ?
7	Des données sensibles, d'infractions ou relatives au NIR sont-elles collectées ? Si oui, les règles spécifiques applicables sont-elles bien respectées ?
8	Y a-t-il des transferts de données en dehors de l'Union européenne ? Si oui, ceux-ci font-ils l'objet d'un encadrement juridique adapté ?
9	Des procédures sont-elles définies afin de respecter les droits des personnes fichées ?
10	Des formalités préalables auprès de la CNIL restent-elles à accomplir en application du droit français ? Y a-t-il des spécificités réglementaires relatives à mon traitement en application du droit français ?