**Article XX – Données personnelles**

En tant que responsable de traitement, XXX s’engage à respecter les obligations de la réglementation européenne et française en matière de protection des données personnelles.

De même, dans le cadre du présent contrat, le sous-traitant s’engage à traiter des données personnelles pour le compte de XXX et dans le respect de la réglementation en vigueur. A cet effet, il s’engage notamment à :

* ne traiter les données personnelles que sur instruction du responsable du traitement, sauf disposition légale ou réglementaire contraire ;
* informer le responsable du traitement dans le cas où le sous-traitant serait soumis à des obligations légales ou réglementaires relatives au traitement de données personnelles ;
* veiller au respect de la confidentialité des données personnelles par ses équipes, personnels ou tiers ;
* veiller à la sécurité du traitement, en prenant notamment toutes les mesures nécessaires pour garantir la sécurité des données personnelles ;
* informer le responsable du traitement en cas de sous-traitance ultérieure, vérifier que le sous-traitant pressenti respecte la réglementation en matière de protection des données personnelles et ne pas recruter un sous-traitant sans l’autorisation écrite préalable du responsable du traitement ;
* aider le responsable du traitement à répondre aux demandes des personnes concernées par un traitement de données personnelles en vue d’exercer leurs droits ;
* aider le responsable du traitement à remplir son obligation de sécurité des traitements et de notification à la CNIL ou aux personnes concernées en cas de violation de données personnelles, notamment en faisant immédiatement remonter au responsable du traitement tout incident ou toute faille de sécurité découverte et susceptible d’impacter des données personnelles ;
* supprimer ou restituer au responsable de traitement les données personnelles à la fin du contrat et au terme de la prestation de services, détruire les copies existantes, sauf disposition légale ou réglementaire contraire ;
* mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article ;
* permettre au responsable de traitement de réaliser des audits pour vérifier la conformité des traitements à la réglementation en matière de protection des données personnelles[[1]](#footnote-1) (ou mettre à la disposition du responsable de traitement tous documents permettant de démontrer la réalisation de contrôles internes pour vérifier la conformité des traitements à la réglementation en matière de protection des données personnelles),
* informer immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation de la réglementation en matière de protection des données personnelles.

1. Cette obligation est très difficile à faire accepter par le sous-traitant, notamment lorsqu’il est situé hors UE, et à réaliser en pratique. Il peut donc être envisagé de l’atténuer en remplaçant la phrase par la phrase surlignée en jaune. [↑](#footnote-ref-1)