**Annexe XX – Traitement des données personnelles**

Dans le cadre du présent contrat, [le prestataire] (ci-après désigné « sous-traitant ») a pour mission de [rappeler objet du contrat] et il est amené, à ce titre, à traiter des données personnelles pour le compte du MEDEF.

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du MEDEF les opérations de traitement de données à caractère personnel.

Dans le cadre de leurs relations contractuelles, les parties s’engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement général sur la protection des données personnelles (RGPD)[[1]](#footnote-1).

1. **Engagements du sous-traitant**

A cet effet, le sous-traitant s’engage à :

* traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance ;
* traiter les données conformément aux instructions du MEDEF. Si le sous-traitant considère qu’une instruction constitue une violation du RGPD ou de toute autre disposition relative à la protection des données, il en informe immédiatement le MEDEF. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis, il doit informer le MEDEF de cette obligation juridique avant le traitement ;
* garantir la confidentialité des données personnelles traitées dans le cadre du présent contrat ;
* veiller à ce que les personnes autorisées à traiter les données personnelles en vertu du présent contrat :

♣ s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

♣ reçoivent la formation nécessaire en matière de protection des données personnelles ;

* prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception (*Privacy by design*) et de protection des données par défaut (*Privacy by default*) ;
* aider le MEDEF pour la réalisation d’analyses d’impact relative à la protection des données et, le cas échéant, pour la réalisation de la consultation préalable de la CNIL ;
* en fonction de l’analyse d’impact, assurer la sécurité des données personnelles et mettre en place les mesures de sécurité appropriées aux risques décelés ;
* mettre à la disposition du MEDEF la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le MEDEF ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
* détruire toutes les données à la fin de la prestation et/ou renvoyer au MEDEF les données personnelles en justifiant de la destruction de toutes les copies existantes dans les locaux ou les systèmes d’information du sous-traitant.

1. **Sous-traitance ultérieure**

[Le prestataire] peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit ou par voie électronique le MEDEF de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le silence du MEDEF dans un délai de 15 jours à compter de la notification du choix du sous-traitant ultérieur vaut acceptation.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient [au prestataire] de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes au regard des exigences du RGPD. Dans le cas contraire, [le prestataire] demeure pleinement responsable devant le MEDEF de l’exécution par l’autre sous-traitant de ses obligations.

1. **Droits des personnes concernées**

Dans la mesure du possible, le sous-traitant doit aider le MEDEF à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées (droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l’objet d’une décision individuelle automatisée).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, celui-ci doit adresser ces demandes dès réception par courrier électronique au MEDEF (indiquer un contact au sein du responsable de traitement).

1. **Notification des violations de données à caractère personnel**

Le sous-traitant notifie au MEDEF toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance. Cette notification doit être faite auprès de (indiquer un interlocuteur privilégié) et être accompagnée de toute documentation utile afin de permettre au MEDEF, si nécessaire, de notifier cette violation à la CNIL.

A la demande du MEDEF, le sous-traitant communique éventuellement, au nom et pour le compte du MEDEF, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

1. **Délégué à la protection des données**

Le cas échéant, le sous-traitant transmet au MEDEF le nom et les coordonnées du délégué à la protection des données qu’il a désigné.

1. Règlement général n° (UE) 2016/679 du 27 avril 2016 relatif à la protection des données personnelles (RGPD). [↑](#footnote-ref-1)