ANNEXE 2 SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Article liminaire

La présente Annexe a pour objet de décrire les obligations respectives des Parties en matière de Données personnelles et fait partie intégrante du CCP.

Les parties contractantes sont :

L'Ined (ci-après, « *le responsable de traitement* ») d'une part,

Et

Le titulaire du marché (et ses sous-traitants éventuels)

(ci-après, « *le sous-traitant* ») d'autre part.

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

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 (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données ») et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte des responsables de traitement les données à caractère personnel nécessaires pour fournir les prestations de services décrites au marché auquel le présent document est annexé.

Les données à caractère personnel désignent toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Les finalités du traitement sont l'impression, la personnalisation, la mise sous pli, le routage et l'expédition des documents pour le compte de l'Ined, ainsi que, le cas échéant, la réalisation de contrôles nécessaires à la bonne exécution des prestations.

Les données à caractère personnel traitées sont les suivantes :

1. Données d'identification : nom, prénom, civilité ;
2. Coordonnées postales : adresse de livraison ou d'expédition, code postal, commune, pays ;
3. Coordonnées professionnelles, le cas échéant : fonction, organisme, service ;
4. Données relatives aux documents à imprimer, lorsqu'elles permettent d'identifier directement ou indirectement une personne ;
5. Données techniques et métadonnées nécessaires à la préparation, au contrôle et au suivi des fichiers et des opérations de routage.

Les catégories de personnes concernées sont notamment les personnes physiques destinataires des documents imprimés et routés dans le cadre du marché, ainsi que, le cas échéant, les personnes dont les coordonnées figurent dans les fichiers transmis par l'Ined au titulaire.

Le responsable de traitement met à la disposition du sous-traitant les informations nécessaires à l'exécution du service objet du présent contrat.

III. Durée du contrat

Le présent contrat entre en vigueur à compter de la notification du présent marché et jusqu'à la date de fin d'exécution des prestations du marché.

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données uniquement pour la finalité qui fait l'objet de la sous-traitance ;

2. Traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit interne, il en informe immédiatement le responsable de traitement. 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 responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel 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 à caractère personnel.

5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

V. Sous-traitance

En cas de recrutement d'un sous-traitant ultérieur, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement.

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 sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

VI. Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise.

La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

VII. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à dpd@ined.fr.

VIII. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais et au plus tard dans un délai de 48 heures après en avoir pris connaissance et par message électronique adressé sur l'adresse du responsable identifié de l'établissement, c'est-à-dire le référent désigné dans l'article VII. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (Commission nationale de l'informatique et des libertés) et, le cas échéant, aux personnes concernées.

IX. Aide apportée par le sous-traitant au responsable de traitement pour le respect de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.
Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

X. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- Le chiffrement des données à caractère personnel lors de la transmission des données afin d'en garantir la sécurité,
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,
- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre.

XI. Sort des données

Au terme de la présente convention, l'accès aux données à caractère personnel est interrompu.
Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à détruire toutes les données à caractère personnel.

XII. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

XIII. Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement conformément aux dispositions prévues au 2 de l'article 30 du règlement général sur la protection des données.

XIV. Documentation
Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

XV. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant,

2. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant,

3. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.