

ANNEXE 10 – LA PROTECTION DES DONNEES DANS LE CAS D'UNE AIDE PERCUE POUR LA REALISATION D'UNE ETUDE

L'article ci-dessous, relatif au RGPD, vient compléter la convention ou décision d'engagement.

Cet article définit les modalités dans lesquelles les membres du groupement traitent chacun des données personnelles pour le compte de l'ODEADOM et la DAAF du département (les « Commanditaires ») et les engagements des Parties afin d'assurer la conformité desdits traitements aux lois et réglementations applicables.

1. Définitions spécifiques

« *Données Personnelles* », « *Données à Caractère Personnel* » ou « *Données* » : désigne toute information concernant une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, 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. Dans le cadre des Traitements de leurs Données Personnelles, les personnes physiques identifiables sont appelées « *Personnes Concernées* ».

« *Traitement* », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données ou des ensembles de Données à Caractère Personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

« *Responsable de Traitement* » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le Responsable de Traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

« *Sous-traitant* » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à Caractère Personnel pour le compte du Responsable du Traitement.

« *Violation de données à caractère personnel* », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à Caractère Personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données.

« *Réglementation applicable* » : désigne toutes les lois et réglementations en relation avec la protection des Données à Caractère Personnel et la vie privée, et notamment la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 modifiée et le Règlement européen n° 2016/679 du 27 avril 2016 dit « Règlement Général sur la Protection des Données » (RGPD).

2. Principes

Dans le cadre de leur partenariat, les Parties s'engagent à respecter la Réglementation applicable. Pour l'application de la convention ou décision d'engagement, le bénéficiaire de l'aide, a accès et traite des Données à Caractère Personnel pour le compte des Commanditaires, considérés comme Responsables de Traitement. A ce titre, ils sont chacun distinctement qualifiés de Sous-traitant, sans que cette qualification commune implique entre eux une idée de solidarité dans les responsabilités associées.

3. Description générale des Traitements

3.1. Description générale des Traitements opérés par le bénéficiaire de l'aide

Les catégories de Données Personnelles traitées sont :

- Les données d'identification : noms complets, localisation et adresses mails et téléphones, des acteurs relatifs au thème de l'étude dans le département dont un registre a été établi sur la base d'un recueil de données publiques disponibles sur internet et d'informations recueillies auprès de certains acteurs enquêtés ou impliqués dans le comité de pilotage de l'étude.
- Les données relatives à la vie professionnelle : caractérisation des métiers dans les entreprises impliquées dans le thème de l'étude
- Les catégories de personnes concernées sont les gestionnaires de contrats publics liés au thème de l'étude
- Les catégories de destinataires des données sont les Commanditaires de l'étude.
- La durée de conservation de ces données est celle de la durée de la convention ou de la décision d'engagement

4. Obligations générales des Sous-traitants

Pour l'exécution la convention ou la décision d'engagement, les membres du Groupement s'engagent chacun à :

- Traiter les Données Personnelles pour les seules finalités qui font l'objet de la sous-traitance les concernant.
- N'agir que sur instructions documentées des Commanditaires en tant que Responsables des Traitements mis en œuvre pour l'exécution du projet. Si le Sous-traitant considère qu'une instruction constitue une violation de la Règlementation Applicable, il en informe immédiatement les Responsables 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'État membre auquel il est soumis, il doit informer les Responsables 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.
- Garantir la confidentialité des Données Personnelles traitées et prendre l'ensemble des mesures d'ordre technique et organisationnel appropriées pour garantir un niveau de sécurité adapté au risque existant afin de prévenir les risques de destruction accidentelle ou illicite, de perte accidentelle, d'altération, de diffusion ou d'accès non autorisés, ainsi que contre toute autre forme de traitement illicite des Données à Caractère Personnel.
- Veiller à ce que les personnes autorisées à traiter les Données Personnelles soient soumises à une obligation appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des Données Personnelles.
- Prendre en compte, s'agissant de ses services, les principes de protection des Données Personnelles dès la conception et de protection des Données Personnelles par défaut.

Les membres du Groupement déclarent chacun tenir par écrit un registre de toutes les catégories d'activités de Traitement effectuées pour le compte des Responsables de Traitement, conformément à la Règlementation applicable.

Les membres du Groupement mettent à la disposition des Responsables de traitement, sur leur demande, la documentation nécessaire pour démontrer le respect de toutes leurs obligations et pour permettre la réalisation d'audits, y compris des inspections, par les Responsables de traitement ou un autre auditeur qu'ils auraient mandaté, et contribuer à ces audits.

5. Obligations des Sous-traitants en cas de sous-traitance ultérieure

Les Sous-traitants peuvent faire appel à un autre sous-traitant (ci-après, « le Sous-traitant Ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, ils informent préalablement les Responsables de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Les Responsables de traitement disposent d'un délai minimum de 10 jours à compter de la date de réception de cette information pour présenter leurs objections, sans quoi la sous-traitance ultérieure est considérée comme autorisée par les Responsables de Traitement dans les termes transmis par le Sous-traitant concerné.

Le sous-traitant ultérieur est tenu de respecter les obligations de la présente clause dans sa mise en œuvre du Traitement opéré pour le compte et selon les instructions des Responsables de Traitement. Il appartient au Sous-traitant initial concerné 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 de la Règlementation Applicable.

6. Obligations d'assistance et de coopération

6.1. Violation de données

Le Sous-traitant concerné notifie aux Responsables de Traitement toute Violation de Données Personnelles dans un délai maximum de 48 heures après en avoir pris connaissance.

La notification devra décrire la nature de la Violation de Données, y compris les catégories et le nombre de Personnes Concernées, le nom de la personne en charge du Traitement concerné, les conséquences de la Violation de Données, les mesures prises pour y remédier, ainsi que le calendrier envisagé pour les mettre en œuvre, en limiter les conséquences, et en prévenir la récurrence. Cette notification est accompagnée de toute la documentation utile afin de permettre aux Responsables de traitement, si nécessaire, de notifier cette Violation à l'autorité de contrôle compétente et aux Personnes Concernées.

Le Sous-traitant concerné s'engage en outre à rechercher l'origine de la violation de données et à mettre en place toutes mesures correctives afin d'y mettre un terme et d'en limiter les conséquences et la récurrence.

Il s'engage également à assister les Responsables de Traitement dans la mise en œuvre des notifications éventuellement nécessaires auprès des autorités compétentes et/ou des Personnes Concernées.

6.2. Information et gestion des demandes d'exercice de droit des Personnes concernées

Chaque membre du Groupement fournit pour les Traitements dont il a la charge aux Personnes Concernées les informations relatives aux finalités et caractéristiques des Traitements de Données à Caractère Personnel objets des présentes, au moment de leur collecte. Ces informations mentionnent notamment les Responsables de Traitement en cette qualité.

Les personnes concernées doivent pouvoir exercer leurs droits d'accès, de rectification, d'effacement, de limitation et d'opposition au traitement, ainsi que de portabilité de leurs Données Personnelles directement auprès des services des Responsables du Traitement.

Dans la mesure du possible, les Sous-traitants doivent aider les Responsables de traitement à s'acquitter de leur obligation de donner suite aux demandes d'exercice des droits des Personnes Concernées, notamment en instaurant toutes les mesures techniques et organisationnelles pertinentes pour en assurer la mise en œuvre effective.

Lorsque les Personnes Concernées exercent auprès de l'un des Sous-traitants des demandes d'exercice de leurs droits, le Sous-traitant concerné adresse ces demandes aux Responsables de Traitement dès qu'il en prend connaissance.

6.3. Analyses d'impact et relation avec l'autorité de contrôle

Les Sous-Traitants s'engagent chacun à coopérer et à assister les Responsables de Traitement pour la mise en œuvre des obligations lui incombant. Plus particulièrement, ils s'engagent :

- A coopérer et assister les Responsables de Traitement, et notamment à fournir tout document et/ou information qui serait nécessaire dans le cadre de la consultation préalable de la CNIL obligatoire en cas de risque résiduel élevé révélé par l'analyse d'impact ;
- A assister les Responsables de Traitement en cas de contrôle et/ou demande de(s) autorité(s) de contrôle (notamment la CNIL).

7. Sort des données personnelles en fin de projet

Au terme du projet (c'est-à-dire à la date de fin de la convention), chaque membre du Groupement doit détruire l'ensemble des Données à Caractère Personnel traitées pour le compte des Responsables de Traitement ainsi que leurs copies existantes dans son système d'information et, le cas échéant, celui de ses sous-traitants ultérieurs.

8. Obligations des Responsables de traitement

Les Responsables de Traitement s'engagent à :

- Fournir aux Sous-traitants l'accès aux Données Personnelles visées à la présente clause lorsque celles-ci sont en possession du responsable de traitement ou que leur accès est conditionné à une action de la part de ce dernier ;
- Documenter par écrit toute instruction concernant le Traitement des Données Personnelles par les Sous-traitants ;
- Veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par la Règlementation Applicable par les Sous-traitants ;
- Superviser le Traitement, y compris réaliser les audits et les inspections auprès des Sous-traitants.