MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Secrétariat général

Direction de l'évaluation de la performance, de l'achat, des finances et de l'immobilier

Service de l'achat, de l'innovation et de la logistique du ministère de l'intérieur

Sous-direction de l'achat et du suivi de L'exécution des marchés

Bureau des achats métiers

ANNEXE 1 AU CCAP : DISPOSITIONS RELATIVES À LA PROTECTION DES DONNÉES PERSONNELLES

Le présent document comprend pages, y compris celle-ci, numérotées de 1 à 7 .

SOMMAIRE

ARTICLE 1. DEFINITIONS SPECIFIQUES 3
ARTICLE 2. DISPOSITIONS RELATIVES A LA PROTECTION DES DONNEES PERSONNELLES. 3
2.1. Description du traitement faisant l'objet de la sous-traitance .. 4
2.2. Sécurité 4
2.3. Obligations du sous-traitant vis-à-vis du responsable de traitement 4
2.3.1. LE SOUS-TRAITANT S'ENGAGE A : 4
2.3.2.LA SOUS-TRAITANCE 5
2.3.3. LE DROIT D'INFORMATION DES PERSONNES CONCERNEES 5
2.3.4. L'EXERCICE DES DROITS DES PERSONNES 5
2.3.5. NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL 6
2.3.6. AIDE DU SOUS-TRAITANT DANS LE CADRE DU RESPECT PAR LE RESPONSABLE DE TRAITEMENT DE CES OBLIGATIONS 6
2.3.7. LE SORT DES DONNEES 6
2.3.8. LE DELEGUE A LA PROTECTION DES DONNEES 6
2.3.9. REGISTRE DES CATEGORIES D'ACTIVITES DE TRAITEMENT 6
2.3.10. DOCUMENTATION 7
2.4. Obligations du sous-traitant vis-à-vis du responsable de traitement 7
2.5. Pénalités applicables 7

ARTICLE 1. DEFINITIONS SPECIFIQUES

Données personnelles : désigne toute information se rapportant à 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 de téléphone, une adresse email, 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.

Traitement : désigne toute opération ou tout ensemble d'opérations qui est réalisé sur les Données à Caractère Personnel, de manière automatisée ou non, tels que la collecte, l'enregistrement, l'organisation, 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, le verrouillage, l'effacement ou la destruction.

Fichier : désigne tout ensemble structuré de Données personnelles, accessible selon les critères déterminés dans la présente Annexe, que cet ensemble soit centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique.

Instruction : désigne toute instruction écrite ou par saisie de données, reçue par le titulaire de la part du Ministère en vertu de l'accord-cadre et notamment de la présente Annexe, et, le cas échéant, des avenants conclus entre le titulaire et le Ministère et ayant pour objet le traitement de Données personnelles.

Responsable de Traitement : désigne 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 ; dans le cadre de l'accord-cadre, le Responsable de Traitement est le Ministère.

Sous-traitant : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données personnelles pour le compte du Responsable du Traitement ; dans le cadre du présent accord-cadre, le Sous-traitant est le titulaire. Le terme de sous-traitant est à ne pas confondre avec le terme de sous-traitant au sens de la réglementation de la commande publique.

ARTICLE 2. DISPOSITIONS RELATIVES A LA PROTECTION DES DONNEES PERSONNELLES

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Dans le cas où le titulaire a accès à des données à caractère personnel lors de la réalisation des prestations, il agit en qualité de sous-traitant au sens de l'article 4 du RGPD, et ce pour le compte de l'administration qui demeure le responsable de traitement.

La présente annexe a 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.

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

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour l'exécution du présent marché, telles que décrites ci-après :

- Les données à caractère personnel nécessaires pour procéder à la mise en place et à la gestion administrative de l'exécution du marché ;
- La nature des opérations réalisées sur les données est la collecte et la consultation ;
- La finalité du traitement est de conserver les coordonnées des agents du responsable de traitement susceptibles d'être contactés par le sous-traitant lors de l'exécution du marché ;
- Les données à caractère personnel traitées sont les noms, prénoms, fonctions, coordonnées professionnelles ;
- Les catégories de personnes concernées sont des agents administratifs ou techniques du responsable de traitement.

2.2. Sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- 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.

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

2.3.1. Le sous-traitant s'engage a :

1. traiter les données uniquement pour la ou les seules finalités qui font 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 des États membres relative à la protection des données, 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 une organisation internationale, en vertu du droit de l'Union ou du droit de l'État 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 marché ;

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :
   - 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.

2.3.2. LA SOUS-TRAITANCE

Le sous-traitant, titulaire du marché, 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 s'engage notamment à présenter à l'administration, les entreprises auxquelles il envisage de confier la réalisation d'activités de traitement spécifiques. Pour ce faire, il remplit une déclaration relative à la présentation d'un sous-traitant ultérieur. Il peut pour cela remplir la rubrique F du formulaire DC4, relative à la sous-traitance de données à caractère personnel. En cas d'accord, l'administration accepte le sous-traitant proposé et agrée ses conditions de paiement dans les conditions prévues aux articles R 2193-1 et s. du code de la commande publique.

En cas de sous-traitance ultérieure, le sous-traitant initial doit inclure dans le contrat de sous-traitance à conclure avec le sous-traitant ultérieur une clause relative aux obligations en matière de protection des données, conformément à l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent marché 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 RGPD. 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.

2.3.3. LE DROIT D'INFORMATION DES PERSONNES CONCERNEES

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

2.3.4. L'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 : 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 (y compris le profilage).

Lorsque les personnes concernées transmettent au sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au représentant du responsable de traitement.

2.3.5. NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et par tout moyen. 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.

2.3.6. AIDE DU SOUS-TRAITANT DANS LE CADRE DU RESPECT PAR LE RESPONSABLE DE TRAITEMENT DE CES OBLIGATIONS

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relatives 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.

2.3.7. LE SORT DES DONNEES

Dans un délai d'un (1) mois calendaire avant la date de fin du marché, le titulaire interroge le responsable de traitement sur le sort des données traitées. Au choix du responsable de traitement, le sous-traitant s'engage à :

- détruire toutes les données à caractère personnel ;
- renvoyer toutes les données à caractère personnel au responsable de traitement ;
- renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

2.3.8. LE DELEGUE A LA PROTECTION DES DONNEES

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.

2.3.9. REGISTRE DES CATEGORIES D'ACTIVITES 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 comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des 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.

2.3.10. DOCUMENTATION

Le sous-traitant met à la disposition du responsable de traitement, dans le délai fixé par la demande, la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

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

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données à caractère personnel nécessaires pour l'exécution du présent accord-cadre ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement de la part du sous-traitant ;
- superviser le traitement, y compris réaliser, le cas échéant des audits et des inspections auprès du sous-traitant.

2.5. Pénalités applicables

En cas de fuite, ou de potentialité de fuite de données personnelles, le sous-traitant encourt, sans mise en demeure préalable, la pénalité mentionnée à l'article 18.4 « Pénalités applicables en cas de fuite ou de potentialité de fuite de données personnelles » du CCAP.