Annexe 1 au Cahier des Clauses Administratives Particulières (CCAP) :

Clause relative au respect du Règlement général sur la protection des données

I) Contexte général

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

Dès la 1ère réunion organisée par l'EdA concernant le respect des données à caractère personnel, seront définies :

- la nature des opérations réalisées sur les données ;
- la ou les finalité(s) du traitement ainsi que les données à caractère personnel traitées ;
- la description des traitements envisagés ;
- les catégories de personnes concernées, le mode de collecte des informations nécessaires à la finalité des prestations, ainsi que les informations nécessaires à la bonne exécution des dispositions prévues ci-dessous ;
- les modalités de traitement des données définies comme « sensibles » ;
- la durée de conservation des données collectées par chacune des parties ;
- les destinataires des données traitées ;
- les sous-traitants intervenant dans le ou les traitement(s), ainsi que leur localisation ;
- les éventuels transferts de données ;
- les mesures de sécurité liées au traitement.

Dans le cadre de leurs relations contractuelles, le titulaire s'engage 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 » ou « RGPD ») et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel .

L'EdA est le responsable du traitement et le titulaire est le sous-traitant des données au sens du règlement susmentionné.

II) Obligations du sous-traitant vis-à-vis de l'EdA

1. Engagement du titulaire

Le titulaire s'engage, pour les bons de commande, et les marchés subséquents notifiés, à :

- respecter les modalités relatives à la sous-traitance ;
- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de prestation au titre du présent accord-cadre ;
- traiter les données conformément aux instructions du responsable du traitement. Si le Titulaire 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 délégué à la protection des données. En outre, si le titulaire 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 le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs significatifs d'intérêt public ;

- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent accord-cadre :
    - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité prévues au CCAP de l'accord-cadre ;
    - reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
    - prennent 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 ;
- mettre en place les outils nécessaires à la protection des données (exemple : logiciel anti-virus), notamment des données définies comme sensibles ;
- informer sans délai l'EdA de toute demande de communication d'informations faite au titulaire et/ou à l'un de ses cotraitant/sous-traitant(s).

Le titulaire communique, à l'EdA, 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. Droit d'information des personnes et exercice des droits des personnes

Le titulaire est tenu de fournir aux personnes concernées par les opérations de traitement, l'information relative aux traitements de données qu'il réalise au moment de la collecte des données.

La formulation et le format de l'information seront convenus avec le délégué à la protection des données avant la collecte de données.

Par ailleurs, le titulaire est tenu d'apporter son aide à l'EdA afin de s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées. Il informe, notamment et dans le cadre de son obligation générale de conseil détaillée au présent document, l'EdA de toute demande liée à l'exercice de ces droits.

3. Notification des violations de données à caractère personnel

Le titulaire notifie, par courriel, à l'EdA, toute violation de données à caractère personnel dès qu'il en a connaissance, et s'engage à permettre à ce dernier de réaliser une notification à la CNIL dans les 72h. Cette notification est accompagnée de toute documentation utile afin de permettre, à l'EdA, de notifier cette violation à l'autorité de contrôle compétente.

Dès lors, la notification contient à minima :

- la description de la nature de la violation de données à caractère personnel, y compris les catégories et le nombre approximatif de personnes concernées par la violation ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du sous-traitant ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le sous-traitant propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Le cas échant, en dehors des cas d'exclusions prévus à l'article 34.3 du RGPD, les individus concernés par la violation de leurs données doivent en être informés par le délégué à la protection des données.

4. Sous-traitance ultérieure de données à caractère personnel

Le sous-traitant remet au responsable de traitement une notification écrite préalable de la désignation de tout nouveau Sous-Traitant Ultérieur, y compris le détail complet du traitement devant être réalisé par le sous-traitant ultérieur. Si dans les 30 jours de la réception de cette notification, le responsable de traitement informe le sous-traitant par écrit de toutes objections (pour des motifs raisonnables) à la désignation proposée :

i. Le sous-traitant travaille de bonne foi avec le responsable de traitement afin de modifier de manière raisonnable d'un point de vue commercial la fourniture des services en évitant le recours au sous-traitant ultérieur ainsi proposé ;

ii. Lorsqu'un tel changement ne peut pas être effectué dans les 30 jours de la réception par le sous-traitant de la notification du responsable de traitement, nonobstant toute disposition contraire du contrat, le responsable de traitement pourra, par notification écrite à l'attention du sous-traitant prenant effet immédiatement, résilier le contrat pour ce qui concerne les services nécessitant le recours au sous-traitant ultérieur proposé.

- Le sous-traitant choisit ce sous-traitant ultérieur avec diligence et prête une attention particulière à sa réputation et à son expérience en matière de fourniture des services sous-traités et au caractère adéquat de ses mesures techniques et organisationnelles. Le sous-traitant conclut un contrat écrit avec tout sous-traitant ultérieur. Ce contrat de sous-traitance ultérieure impose au sous-traitant ultérieur des obligations aussi protectrices des données personnelles que celles imposées au sous-traitant. En ce qui concerne les services sous-traités, sont décrits les services sous-traités, et décrites les mesures techniques et organisationnelles que le sous-traitant ultérieur doit mettre en œuvre, et qui s'appliquent aux services sous-traités. A la demande du responsable de traitement et dans un délai raisonnable, le sous-traitant fournit une copie du contrat de sous-traitance ultérieure.

- Pendant toute la durée du marché, sans frais pour le responsable de traitement, le sous-traitant contrôle activement, audite régulièrement et le cas échéant, prend des mesures pour que chaque sous-traitant ultérieur se conforme à ses obligations et signale dans les meilleurs délais au responsable de traitement tout manquement aux dispositions du présent marché, détecté ou signalé par le sous-traitant ultérieur et toutes mesures prises pour y remédier.

- En cas de manquement, les parties négocient de bonne foi afin de déterminer si et comment le sous-traitant peut poursuivre la fourniture des services sans le sous-traitant ultérieur en question. Si les parties sont dans l'incapacité de convenir d'une solution mutuellement acceptable, le responsable de traitement peut résilier les services concernés moyennant un préavis écrit raisonnable.

- Si un sous-traitant ultérieur se trouve en dehors de l'UE / EEE, dans un pays non reconnu comme offrant un niveau de protection des données adéquat, le sous-traitant doit fournir, sur demande, au responsable de traitement les autres informations et la documentation pertinente sur le système de transfert international des données conformément à l'Art. 46 du RGDP qui est utilisé pour divulguer légalement les données à caractère personnel du responsable de traitement au sous-traitant.

5. Audit

Le responsable de traitement peut soumettre à tout moment le sous-traitant à un audit de sécurité en vertu de l'article 28 (h) du RGPD dans le but de vérifier la conformité du traitement de données à caractère personnel aux dispositions de la présente clause, et notamment, mais sans que cela soit limitatif, peut inspecter les bureaux, installations, équipements, systèmes informatiques, éléments techniques, politiques, contrôles et pratiques du sous-traitant en matière de protection de données à caractère personnel en lien avec le présent contrat, sous réserve d'en informer le sous-traitant par écrit au minimum quinze (15) jours avant la date d'audit prévue.

Dans ce cadre, le responsable de traitement peut notamment tester les méthodes de travail du personnel du sous-traitant, vérifier les registres, et le sous-traitant doit fournir au responsable de traitement tout document ou toute information en rapport avec le traitement de données à caractère personnel sous-traité. Sauf en cas de justification écrite du Sous-traitant, celui-ci doit permettre tous accès requis par le responsable de traitement pendant les jours ouvrables aux différents lieux concernés par l'exécution du présent marché.

L'audit peut être effectué par le responsable de traitement ou toute personne tierce habilitée par lui, et dure le temps nécessaire pour effectuer un audit complet.

Le responsable de traitement remet au sous-traitant dans un délai de trente (30) jours à compter de la date de fin de l'audit un rapport sur les résultats de l'audit faisant apparaître tous points critiques et/ou de non-conformité.

Si les conclusions de l'audit révèlent des défaillances, le sous-traitant doit définir et mettre en œuvre, à ses frais, des plans d'actions correctives. La définition du contenu des plans d'actions correctives est réalisée en concertation entre les parties et les coûts de mise en œuvre de ces mesures correctives sont à la charge du sous-traitant sauf accord contraire et écrit des parties.

En toute hypothèse, le responsable de traitement cherche à limiter l'impact de l'audit sur l'activité quotidienne du sous-traitant.

6. Mesures de sécurité

Le titulaire s'engage à mettre en œuvre les mesures de sécurité décrites dans son offre et qui répondent aux obligations suivantes :

- 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.

7. Traitement des données à échéance des prestations

Le titulaire est tenu de certifier que les documents et informations en sa possession, concernant les services réalisés dans le cadre du présent contrat ainsi que toutes les données à caractère personnel manipulées, sont supprimées de tout support informatique et qu'aucune édition ou copie n'est conservée par le titulaire à l'issue du contrat. Ces destructions et non conservations sont formalisées au travers d'un certificat.

8. Registre des catégories d'activité du traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'EdA comprenant notamment :

- le nom et les coordonnées du responsable du 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 à 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, l'anonymisation 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.

9. Documentation

Le titulaire met à disposition de l'EdA la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris par un tiers.