

## **ANNEXE 3 – TRAITEMENT DES DONNEES PERSONNELLES**

### **Loi n° 78-17 - R.G.P.D.**

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire du marché public s'engage à effectuer pour le compte de l'acheteur les opérations de traitement de données à caractère personnel définies ci-après.

Chaque Partie doit en tout temps respecter la Règlementation Données qui lui est applicable et mettre l'autre Partie en situation de respecter ses propres obligations.

A ce titre, chaque Partie s'engage notamment à mettre en oeuvre, à ses frais, les obligations décrites dans la présente annexe et à les faire respecter par quiconque à qui elle donne accès à tout ou partie des Données Personnelles.

Dans le cadre du présent marché public, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le RGPD et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En application de l'article 13 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), les titulaires sont informés que des données à caractère personnel (notamment nom, prénom, adresse mail, données de connexion) collectées dans le cadre de l'exécution du présent accord cadre sont susceptibles de faire l'objet de traitement(s).

Pour l'application de la présente annexe, le responsable de traitement au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après, « règlement général sur la protection des données » ou RGPD) est l'acheteur et le sous- traitant est le titulaire du marché public.

Identité et coordonnées du responsable de traitement et de son représentant :

Le Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique (MEFSIN), ci-après « l'Acheteur »

59, boulevard Vincent Auriol

75703 Paris Cedex 13

Responsable de Traitement Opérationnel (RTO) : L'Agence française anticorruption, représentée par le Directeur de de l'Agence française anticorruption.

Coordonnées du délégué à la protection des données :

[le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr](mailto:le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr)

Bases juridiques du traitement :

- c) et e) de l'article 6.1 du RGPD

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

## A. CADRE DEFINI PAR L'ACHETEUR

### ARTICLE PRELIMINAIRE. DEFINITIONS SPECIFIQUES ET CADRE DU TRAITEMENT

Pour les besoins de la présente annexe, les Parties conviennent des définitions spécifiques suivantes :

« Acheteur »	désigne le MEFSIN
« Donnée Personnelle »	désigne toute information se rapportant à une Personne identifiée ou identifiable. Est réputé identifiable la Personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques propres à son identité.
« EEE »	désigne l'Espace Economique Européen comprenant, à la date du Marché, l'Union européenne, la Norvège, l'Islande et le Liechtenstein.
« Garanties »	désigne les garanties appropriées prises pour préserver la sécurité et la confidentialité des Données Personnelles Transférées hors de l'EEE, dans un pays dont la législation n'a pas été reconnue adéquate par les autorités européennes, dans les conditions prévues par la Réglementation Données.
« Réglementation Données »	désigne la réglementation applicable à l'AFA en matière d'utilisation de Données Personnelles, et en particulier la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que toute réglementation destinée à la compléter ou à la remplacer, en particulier, le Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
« Personne »	désigne toute personne physique (client, salarié, prestataire, fournisseur...) dont les Données Personnelles sont susceptibles de faire l'objet d'un Traitement dans le cadre de l'accord-cadre
« Prestataire »	désigne le Titulaire de l'accord-cadre.
« Responsable du Traitement »	désigne la Partie qui détermine, seule ou conjointement avec un autre Responsable de Traitement, les finalités et les moyens d'un Traitement, dont il peut être amené à confier la réalisation en tout ou partie à un ou plusieurs Sous-Traitants. En l'espèce l'Acheteur est le responsable de traitement. L'AFA est le responsable de traitement opérationnel.
« Sous-Traitant »	désigne toute personne physique ou morale amenée à Traiter des Données Personnelles pour le compte d'un Responsable du Traitement.

« Traitement » ou « Traiter »	désigne le fait de réaliser toute opération ou série d'opérations portant sur des Données Personnelles, telle que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction, indépendamment du fait que cette opération est réalisée automatiquement ou pas.
« Transfert » ou « Transférer »	désigne le fait de transférer des Données Personnelles ou d'y donner accès, y compris par simple mise à disposition, depuis le territoire d'un pays de l'EEE vers un pays situé hors de l'EEE.

## ARTICLE 1. AUTORISATION DE TRAITEMENT

Dans le cadre de l'exécution des prestations prévues à l'accord-cadre, l'AFA donne la possibilité au prestataire, pendant toute la durée de l'accord-cadre et jusqu'à l'expiration des durées qu'elle a définies, d'avoir accès aux Données Personnelles pour le compte de l'Agence, dans les conditions décrites ci-dessous :

Finalités des Traitements mis en oeuvre par le Prestataire	Finalité 1 : Assistance à l'AFA dans l'exercice de ses missions de contrôle, par la réalisation de prestations spécifiques précisées à l'accord-cadre,
Catégories de Données Personnelles Traitées par le Prestataire	Le prestataire peut avoir accès à des données personnelles des entités contrôlées exclusivement par les deux voies suivantes : - données transmises par l'AFA ; - données récupérées par le prestataire directement auprès des entités, uniquement sur consigne ou après validation préalable de l'AFA. Les « catégories de données personnelles traitées » dans ce cadre s'entendent de toute information se rapportant à une Personne identifiée ou identifiable. Est réputé identifiable la Personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques propres à son identité.
Catégories de Personnes	Collaborateurs de l'entité objet de la mission, clients, fournisseurs, intermédiaires.
Durée de conservation	Pendant la durée de la prestation : A l'issue du délai d'un mois après la fin de la prestation, -sauf indication particulière de l'AFA-, l'intégralité des données doit être restituée à l'AFA dans un format exploitable. Conformément à l'article 9.2 de la présente annexe, le prestataire s'engage à ne conserver aucune copie, quel qu'en soit le support. De plus, à l'issue de l'accord-cadre, le prestataire confirme expressément à l'AFA avoir restitué

	l'ensemble des Données auxquelles il a eu accès et n'en avoir conservé aucune copie.
--	--

## **ARTICLE 2. OBLIGATIONS GENERALES DE L'AFA**

2.1 L'AFA indique au Prestataire les modes opératoires envisageables pour la transmission sécurisée des données ; si en cours de prestation le mode opératoire utilisé ne convient plus ou dysfonctionne, tout autre mode opératoire envisagé doit être préalablement validé par l'AFA.

2.2 Droit d'information et exercice des personnes concernées par le traitement (Option 1) : Il appartient à l'AFA de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Conformément aux dispositions des articles 15 à 21 du RGPD, les personnes dont les données à caractère personnel sont collectées disposent notamment d'un droit d'accès, de rectification et d'effacement à ces informations qui les concernent, sous réserve des limitations éventuelles posées par les textes. De même, elles peuvent également s'opposer au traitement de ces données, sous les mêmes réserves.

L'exercice des droits d'information et d'accès aux données à caractère personnel peut être effectué auprès du délégué à la protection des données.

La personne dont les données à caractère personnel sont collectées dans le cadre de la présente procédure dispose d'un droit de réclamation auprès de la CNIL

Dans ce cadre, le Prestataire agit en qualité de Sous-Traitant de l'Acheteur ; il reconnaît ne disposer d'aucun droit sur les Données Personnelles qu'il Traite pour le compte de l'AFA.

## **B. OBLIGATIONS DU PRESTATAIRE ET, LE CAS ECHEANT, DE SON SOUS-TRAITANT AU SENS DU CODE DE LA COMMANDE PUBLIQUE**

2.1 Le Titulaire ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

2.2 Le Prestataire s'engage à se conformer aux instructions écrites de l'AFA s'agissant de l'utilisation qui peut être faite des Données Personnelles.

Le Prestataire s'interdit donc en particulier de réaliser tout Traitement utilisant les Données Personnelles, qui ne serait pas expressément demandé par l'AFA dans le cadre d'une instruction documentée.

2.3 Le Prestataire informera immédiatement l'AFA si, selon lui, une de ses instructions est susceptible de constituer une violation de la Règlementation Données.

### **ARTICLE 3. MESURES DE SECURITE**

3.1 Le Prestataire s'engage à mettre en oeuvre des mesures techniques et organisationnelles appropriées, précises, détaillées et documentées pour protéger les Données Personnelles contre tout risque de destruction, perte, altération, divulgation ou accès non autorisé, aux Données Personnelles, mais également pour en assurer la disponibilité et l'intégrité. Ces mesures techniques et organisationnelles devront impérativement être décrites dans l'offre technique du Prestataire.

3.2 Afin de garantir un niveau de sécurité adapté, le Prestataire mettra notamment en oeuvre, en tenant compte des risques pour la sécurité des Données Personnelles et pour la vie privée des Personnes, les mesures techniques et organisationnelles appropriées telles que :

- (i) la pseudonymisation ou le chiffrement des Données Personnelles et/ou des supports ;
- (ii) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de Traitement ;
- (iii) des moyens permettant de rétablir la disponibilité des Données Personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- (iv) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

3.3 Le Prestataire est informé que la sécurité des Données Personnelles auxquelles il a accès est d'une importance cruciale pour l'Acheteur. Le Prestataire déclare être en mesure de garantir un niveau de sécurité adapté afin d'assurer la protection des Données Personnelles dans le cadre des règles relatives à la protection des données applicables au présent marché.

### **ARTICLE 4. CONFIDENTIALITE**

4.1 Sans préjudice de l'article 9.11 du CCP « Confidentialité et secret des affaires », le Prestataire respectera les obligations de confidentialité suivantes :

- (i) ne prendre aucune copie des documents et supports d'informations comportant des Données Personnelles ou des Données Personnelles elles-mêmes, à l'exception de celles strictement nécessaires pour les besoins de l'exécution de sa prestation, objet du Marché ;
- (ii) ne pas utiliser les documents et Données Personnelles à des fins autres que celles spécifiées au Marché ;
- (iii) ne pas divulguer ces documents ou Données Personnelles à des tiers non autorisés, y compris au sein du groupe de sociétés auquel il appartient.

4.2 Le Prestataire n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Il s'engage à soumettre son personnel autorisé à Traiter les Données Personnelles :

- (i) à un devoir de confidentialité et à en assurer le respect, au besoin au moyen de sanctions disciplinaires ;
- (ii) à des formations spécifiques en matière de protection des Données Personnelles.

De manière générale, le Prestataire devra intégrer la protection de la vie privée dans la conception et tout au long de la fourniture de ses services.

## **ARTICLE 5. NOTIFICATION DES FAILLES DE SECURITE**

5.1 En cas de faille de sécurité de nature à affecter la sécurité des Données Personnelles (même si le risque ne s'est pas encore réalisé), le Prestataire s'engage à :

- (i) en notifier par écrit l'existence à l'Acheteur et au plus tard 24 heures après sa survenance ; La notification contient au moins :
  - la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
  - le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
  - la description des conséquences probables de la violation de ces données à caractère personnel ;
  - la description des mesures prises ou que l'Acheteur 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.
- (ii) procéder aux investigations permettant de fournir par écrit, au fur et à mesure de leur réalisation, à l'Acheteur toute information utile sur la nature et l'étendue des Données Personnelles éventuellement déjà touchées et les mesures correctrices prises ou envisagées ;
- (iii) mettre immédiatement en place les mesures correctrices pour empêcher qu'une telle faille puisse perdurer et/ou se reproduire et réparer les conséquences dommageables.

5.2 Cette notification est accompagnée de toute documentation utile afin de permettre à l'Acheteur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance.

## **ARTICLE 6. SOUS-TRAITANCE ULTERIEURE ET CESSIION DE DROITS ET OBLIGATIONS**

6.1 Lorsque le Prestataire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit l'Acheteur. Cette information doit indiquer clairement la nature des activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Cette sous-traitance ne peut être effectuée que si l'Acheteur n'a pas émis d'objection pendant le délai de 21 jours à compter de la date de réception de la demande en application des dispositions de l'article R. 2193-4 du code de la commande publique.

Afin d'obtenir l'acceptation et l'agrément de l'Acheteur le Prestataire doit présenter son sous-

traitant par le biais de l'acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent (téléchargeable sur <https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat>).

6.2 Le sous-traitant du Prestataire est tenu de respecter les obligations du présent accord-cadre pour le compte et selon les instructions de l'AFA. Il appartient au Prestataire de s'assurer que le sous-traitant 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 législation et de la réglementation en vigueur sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant l'AFA de l'exécution par le sous-traitant de ses obligations. Le Prestataire informe préalablement et par écrit l'AFA de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants

## **ARTICLE 7. TRANSFERT DE DONNEES PERSONNELLES HORS EEE**

7.1. Si le Prestataire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) 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 préalablement l'AFA de cette obligation. L'AFA s'assurera de la conformité de ce transfert avec la Loi n° 68-678 du 26 juillet 1968 dite « de blocage ».

Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé.

7.2. A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le Prestataire suspend tout transfert et se rapproche de l'AFA pour envisager, le cas échéant, l'adaptation des modalités d'exécution de l'accord-cadre permettant le respect des exigences du RGPD.

Si les modalités d'exécution ne peuvent être adaptées, l'Acheteur procède, sur demande de l'AFA, à la résiliation l'accord-cadre pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.

## **ARTICLE 8. OBLIGATION DE COOPERATION DU PRESTATAIRE**

8.1 Le Prestataire s'engage à apporter toute l'assistance nécessaire à l'AFA afin de lui permettre de respecter toutes ses obligations en vertu de la Réglementation Données, notamment pour lui permettre de réaliser les analyses et autres consultations requises ou encore pour permettre aux Personnes d'exercer leurs droits sur leurs Données Personnelles. Dans ce dernier cas, si le Prestataire reçoit directement des demandes de Personnes, il s'engage à les transmettre à l'Acheteur sans délai à l'adresse suivante : [le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr](mailto:le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr)

8.2 Le Prestataire s'engage également à coopérer avec l'autorité de contrôle compétente, ce qu'il s'oblige à ne faire qu'après concertation avec l'Acheteur.

8.3 Le Prestataire tiendra à disposition de l'Acheteur et de l'AFA et leur communiquera à première demande toutes les preuves du respect de ses obligations en vertu de la Règlementation Données, et en particulier, au plus tard à compter de l'entrée en application de cette obligation, une copie du registre de toutes les catégories d'activités de Traitement effectuées pour le compte de l'AFA.

8.4 Afin de permettre à l'AFA de s'assurer du respect de ses obligations au titre de la présente annexe, le Prestataire :

- (i) effectuera au moins une fois par an, au plus tard à la date anniversaire du Marché, un audit de ses systèmes d'information et remettra à l'Acheteur un rapport écrit de cet audit ;
- (ii) permettra à l'AFA d'organiser tout audit de ses systèmes d'information et de ses procédures, sous réserve d'en avoir été informé avec un préavis d'au moins 48 heures.

8.5 Si un des rapports d'audit effectué laisse apparaître un ou des manquements du Prestataire à l'une de ses obligations en vertu de la présente annexe, l'AFA pourra, à son choix, demander au Prestataire de mettre immédiatement en place les mesures correctrices pour réparer son ou ses manquement(s) et en réparer les conséquences dommageables, ou résilier le Marché de plein droit dans les conditions prévues à l'article 11.2.

## **ARTICLE 9. DUREE DE CONSERVATION DES DONNEES PERSONNELLES**

9.1 Si le Prestataire est amené à stocker les Données Personnelles, il s'engage à appliquer les durées de conservation et d'accès déterminées par l'AFA.

9.2 A l'issue des durées définies, mais également à la fin de l'accord-cadre, le Prestataire s'engage à restituer, selon les modalités prescrites par l'AFA, tous fichiers comportant des Données Personnelles. Il s'engage à n'en conserver aucune copie, sous quelque support que ce soit.

9.3 Le Prestataire devra justifier à première demande du Pouvoir Adjudicateur du respect de ces obligations.

## **ARTICLE 10. DELEGUE A LA PROTECTION DES DONNEES PERSONNELLES**

Le Prestataire communique à l'AFA les coordonnées de son délégué à la protection des Données Personnelles, s'il en a désigné un, au plus tard une semaine après l'entrée en vigueur de la présente annexe puis, après chaque modification desdites coordonnées.

## **ARTICLE 11. MANQUEMENT A LA PRESENTE ANNEXE**

11.1 En cas de manquement par le Prestataire à l'une de ses obligations au titre de la présente annexe, il s'engage à mettre en oeuvre toute mesure correctrice requise dans les délais et conditions fixées par l'AFA, et ce sans surcoût pour ledit acheteur.

11.2 Au surplus, nonobstant toute clause contraire du Marché, il est expressément convenu qu'en cas de manquement à l'une des obligations prévues dans la présente annexe :

L'AFA pourra, 72 heures après mise en demeure notifiée par tout moyen au Prestataire, ou immédiatement en cas de manquement non réparable, résilier le Marché de plein droit



nonobstant le droit de demander indemnisation du préjudice subi pour les dommages directs et réels au sens des articles 1231-3 et suivants du Code civil résultant desdits manquements. Sont notamment considérés comme des dommages directs :

- a. Les coûts liés à la mise en oeuvre de mesures palliatives visant à remédier à toute défaillance importante du Prestataire afin de se conformer à ses obligations ;
- b. Les coûts supplémentaires encourus par l'AFA pour obtenir des services similaires auprès d'un tiers que le Prestataire n'est pas en mesure de fournir ;
- c. Les coûts de personnel connexes (salaires, heures supplémentaires, recours à du personnel supplémentaire), les coûts de télécommunication et les autres coûts de même nature engagés par l'AFA pour mettre en oeuvre tout ou partie des obligations du Prestataire défaillant ; et
- d. Les coûts de rechargement ou de récupération des Données Personnelles auxquelles le prestataire aura eu accès dans l'exercice de ses prestations.

Le Prestataire ne pourra pas prétendre au bénéfice de toute clause du Marché pouvant avoir pour objet ou pour effet d'exclure ou de limiter sa responsabilité pour les préjudices directs subis par l'Acheteur au titre d'un manquement ou d'une négligence en matière de protection des Données Personnelles.

## **ARTICLE 12. DONNEES PERSONNELLES COMMUNIQUEES PAR LE PRESTATAIRE AU POUVOIR ADJUDICATEUR**

12.1 Le Prestataire pourra donner accès à des Données Personnelles concernant son personnel à l'AFA. Celui-ci les Traitera pour les besoins du suivi du Marché en qualité de Responsable du Traitement opérationnel. Le Prestataire garantit que ces Données Personnelles ont été collectées et traitées en conformité avec la Règlementation Données, et fait son affaire notamment (i) de procéder à toutes les formalités préalables qui lui incombent en vertu de la Règlementation Données et (ii) d'informer pour le compte de l'AFA les Personnes du Traitement par ledit acheteur de leurs Données Personnelles, dans les conditions prévues par la Règlementation Données.

12.2 A cette fin, le Prestataire est informé que les Personnes concernées par de tels Traitements réalisés par l'AFA peuvent exercer les droits qui leur sont garantis par la Règlementation Données, par email à l'adresse suivante : [le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr](mailto:le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr)