**Annexe 1 au CCAP encadrant la sous-traitance des traitements de données à caractère personnel**

(*Les soumissionnaires sont invités à compléter et modifier, le cas échéant, la présente annexe*)

**« 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; 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 du 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.

***Pour le présent marché, le responsable de traitement au sens du RGPD est l’IRD*.**

**« Titulaire » :** désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données Personnelles pour le compte, sur instruction et sous l’autorité de l’IRD.

**« Destinataire » :** désigne la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui reçoit communication de Données Personnelles, qu’il s’agisse ou non d’un tiers.

**« Données Personnelles » ou « Données à caractère personnel**»: désigne 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.

**« Finalité(s) » :** désigne l’objectif principal d’un Traitement de Données à caractère personnel.

**« Personne(s) concernée(s) » :** désigne les personnes physiques identifiables ou identifiées dont les Données Personnelles sont collectées et intégrées dans le Traitement.

**« Autorité(s) de contrôle » :** désigne l’(les) autorité(s) publique(s) indépendante(s) instituée(s) par chaque État membre chargée(s) de surveiller l'application du Règlement Européen sur la Protection des Données, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des Données Personnelles au sein de l'Union européenne.

**« Analyse d’impact » :** désigne un processus dont l’objet est de décrire le Traitement de données à caractère personnel, d’en évaluer la nécessité ainsi que la proportionnalité et d’aider à gérer les risques pour les droits et libertés des personnes physiques liés au Traitement de leurs Données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face.

**« Traitement de données à caractère personnel » ou « Traitement » :** désigne toute opération ou ensemble d’opérations portant sur des Données Personnelles, quel que soit le procédé utilisé telles que la collecte, l’enregistrement, l’organisation, la conservation, 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.

**« Violation » :** désigne une faille de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles.

**« Transfert » :** désigne toute communication, copie ou déplacement de Données Personnelles ayant vocation à être traitées dans un pays tiers à l’Union européenne et n’ayant pas un niveau de protection adéquat ou dans une organisation internationale.

**« Règlement européen » ou « Règlement européen sur la Protection des Données » :** désigne le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 applicable à compter du 25 mai 2018.

**« Marché » :** désigne les lots sur lesquels le soumissionnaire souhaite présenter une offre […].

**« Délégué » :** désigne le (la) délégué(e) à la protection des Données Personnelles tel que défini par la section 8 du Règlement européen sur la Protection des Données.

1. **Objet**

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire effectue pour le compte de l’IRD 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 »).

## **Description du traitement faisant l’objet du transfert des données à caractère personnel**

Le Titulaire est autorisé à traiter pour le compte de l’IRD les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

|  |
| --- |
| Prestations entrainant le traitement de données : XXXXXXXXXX |
| Description des opérations réalisées sur les données : XXXXXXXXXX |
| Finalité(s) du traitement : XXXXXXXXXX |
| Type de données à caractère personnel traitées : XXXXXXXXXX |
| Catégories de personnes concernées : XXXXXXXXXX |
| Durée de conservation des données : XXXXXXXXXX |
| Base légale du traitement : XXXXXXXXXX |
| Nécessité de copier des données dans le système informatique du Titulaire : OUI / NON |
| Conservation de copies : XXXXXXXXXX |
| Intervenants sous-traitants du Titulaire : OUI / NON  Si oui, identité, coordonnées et missions : XXXXXXXXXX |
| Applications concernées : XXXXXXXXXX |
| Sort des données au terme du traitement : XXXXXXXXXX |
| Autres précisions ou interdictions : XXXXXXXXXX |

Toute intervention ponctuelle et supplémentaire non prévue dans le marché et nécessitée sur les données objet de la présente annexe devra faire l’objet d’instructions documentées de la part de l’IRD dans les mêmes modalités que le tableau ci-dessus préalablement à toute intervention du Titulaire.

1. **Obligations du Titulaire vis-à-vis de l’IRD**

Le Titulaire s'engage à :

* 1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la prestation;
  2. traiter les données conformément aux instructions documentées de l’IRD. 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 Etats membres relative à la protection des données, il en informe immédiatement l’IRD. 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’Etat membre auquel il est soumis, il doit informer l’IRD de cette obligation juridique avant le transfert, 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 toutes les mesures utiles en vue d’assurer la sécurité des données conformément à l’article 32 du règlement européen sur la protection des données et ainsi 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

## Sous-traitance

Le Titulaire est autorisé à faire appel à un sous-traitant ultérieur pour mener les activités de traitement suivantes :

- XXXXXXXXXXXXXXXXX

- XXXXXXXXXXXXXXXXX

Le Titulaire informe préalablement et par écrit l’IRD des coordonnées du ou des sous-traitants ultérieurs au(x)quel(s) il recourt ainsi que de tout changement envisagé concernant l’ajout ou le remplacement d’un sous-traitant ultérieur. Cette information doit clairement indiquer les activités de traitement sous-traitées, l’identité et les coordonnées de ce sous-traitant ultérieur et les date du contrat liant le Titulaire à ce sous-traitant. L’IRD dispose d’un délai de sept (7) jours calendaires à compter de la réception de cette information pour présenter ses objections. Le cas échéant, le Titulaire ne pourra pas effectuer la sous-traitance.

Le sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions de l’IRD. Il appartient au Titulaire 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 du règlement européen sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Titulaire demeure pleinement responsable devant l’IRD de l’exécution par le sous- traitant de ses obligations.

## Exercice des droits des personnes

Dans la mesure du possible, le Titulaire doit aider l’IRD 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).

Le Titulaire doit transmettre à l’IRD l’ensemble des demandes d’exercice de droits qui lui sont adressées directement s’agissant des données faisant l’objet de la prestation prévue par le présent marché dans les sept (7) jours calendaires suivants cette demande afin de permettre à l’IRD d’y répondre dans les délais prévus par le règlement européen sur la protection des données.

## Notification des violations de données à caractère personnel

Le Titulaire notifie à l’IRD toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance en adressant un email avec accusé de réception à : [dpd@ird.fr](mailto:dpd@ird.fr). Cette notification est accompagnée de toute documentation utile afin de permettre à l’IRD, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente et, le cas échéant,aux personnes concernées.

## Aide du Titulaire dans le cadre du respect par l’IRD de ses obligations

Le Titulaire s’engage à aider l’IRD à garantir le respect des obligations relatives à la sécurité des données.

Le Titulaire aide l’IRD, le cas échéant, pour la réalisation d’analyses d’impact relative à la protection des données.

Le Titulaire aide l’IRD, le cas échéant, pour la réalisation de la consultation préalable de l’autorité de contrôle.

## Mesures de sécurité

Le Titulaire s’engage à tenir compte de la nature du traitement et à mettre en œuvre les mesures de sécurité suivantes :

|  |  |
| --- | --- |
| Pseudonymisation des données à caractère personnel (si applicable) | A compléter par l’IRD ou par le titulaire |
| Chiffrement des données à caractère personnel | A compléter par l’IRD ou par le titulaire |
| Moyens permettant de garantir la confidentialité et l’intégrité des données | A compléter par l’IRD ou par le titulaire |
| Moyens permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés en cas d’incident physique ou technique | A compléter par l’IRD ou par le titulaire |
| Procédure visant à tester, analyser, évaluer l’efficacité des mesures de sécurité | A compléter par l’IRD ou par le titulaire |

* 1. Sort des données

Au terme du marché, le Titulaire s’engage à renvoyer toutes les données à caractère personnel à l’IRD sauf instruction différente reçue de l’IRD. Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du Titulaire, sauf si le droit de l’Union Européenne ou le droit français n’exige la conservation des données en cause. Une fois détruites, le Titulaire doit justifier par écrit à l’IRD, sous la forme d’une attestation signée du Titulaire, de la destruction.

## Délégué à la protection des données

Le Titulaire communique à l’IRD 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. S’il n’en n’a pas désigné, il en explique les raisons à l’IRD.

## Registre des catégories d’activités de traitement

Le Titulaire déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte de l’IRD comprenant les éléments imposés par le règlement européen sur la protection des données.

## Documentation - Audit

Le Titulaire met à la disposition de l’IRD la documentation nécessaire pour démontrer le respect de toutes ses obligations prévues à la présente annexe et plus généralement le respect de toutes ses obligations en matière de protection de données à caractère personnel ainsi que pour permettre la réalisation d'audits, et contribuer à ces audits.

Le Titulaire autorise l’IRD, notamment son Délégué, ou tout autre auditeur externe non concurrent du Titulaire et mandaté par le Délégué de l’IRD à inspecter et auditer les activités de traitements qui lui sont sous-traitées en application des présentes et s’engage à accéder à toutes demandes raisonnables émises par l’IRD afin de vérifier que le Titulaire respecte les obligations mises à sa charge par la présente annexe. En cas d’audit, l’IRD devra en informer le Titulaire au moins quinze (15) jours à l’avance, et l’audit sera circonscrit aux traitements sous-traités en application de la présente annexe.

Le Titulaire coopérera avec l’IRD et ses représentants pour l’accès aux locaux, aux informations nécessaires et à ses employés dans la mesure où l’audit l’exige.

Les personnes mandatées pour réaliser l’audit se soumettront préalablement à un accord de confidentialité des informations auxquelles elles accèderont au cours de l’audit.

En revanche, les audits de contrôle faisant suite à des dysfonctionnements non résolus et à des inspections à l’initiative d’une autorité de contrôle ne sont pas soumis aux restrictions détaillées ci-dessus.

## **Obligations de l’IRD vis-à-vis du Titulaire**

L’IRD s’engage à :

* 1. Fournir au Titulaire les données visées au II des présentes clauses ;
  2. Documenter par écrit toute instruction concernant le traitement des données par le Titulaire ;
  3. 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 Titulaire ;
  4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire ;
  5. Informer les personnes concernées des opérations de traitement, notamment celles visées à la présente annexe, au moment de la collecte des données ;
  6. Notifier, le cas échéant, les violations de données à caractère personnel qui lui auront été communiquées par le Titulaire à l’autorité de contrôle compétente ainsi qu’aux personnes concernées, dans le respect des articles 33 et 34 du RGPD ;
  7. Donner suite aux demandes d’exercice des droits des personnes concernées directement adressées à l’IRD ou dûment communiquées dans les délais par le Titulaire.