**Annexe de sous-traitance**

**Traitement de données comportant des informations à caractère personnel**

**Marché « Suivi du potentiel écotoxique des estuaires du bassin Seine-Normandie : analyses écotoxiques sur matrice sédiment dans les estuaires du bassin »**

**Entre :**

**L’Agence de l’eau Seine-Normandie**

Représentée par sa Directrice générale, Sandrine ROCARD, et désigné ci-après par le terme « le Responsable du traitement », d’une part,

**Et**

**………………………………………………………………**

Représentée par Monsieur / Madame ………………………………. au sens de l’article 4.8 du règlement général sur la protection des données (RGPD) et désigné ci-après par le terme « le Sous-traitant », d’autre part,

**Préambule, au sens du RPGD :**

Le Responsable de traitement au sens de l’article 4.7 du règlement général sur la protection des données (RGPD) est l’Agence de l’eau Seine-Normandie, acheteur public. Le Sous-traitant est le titulaire du présent marché.

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 »).

# ARTICLE 1 - Objet

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 dans le cadre de l’exécution des prestations ci-après définies : suivi du potentiel écotoxique des estuaires du bassin Seine-Normandie : analyses écotoxiques sur matrice sédiment dans les estuaires du bassin.

# ARTICLE 2 - Description du traitement

⮚ Le Sous-traitant est autorisé à traiter pour le compte du Responsable de traitement, les données à caractère personnel nécessaires pour fournir la prestation suivante : suivi du potentiel écotoxique des estuaires du bassin Seine-Normandie : analyses écotoxiques sur matrice sédiment dans les estuaires du bassin.

⮚ La nature des opérations réalisées sur les données à caractère personnel est : consultation et utilisation de données dans le cadre du suivi du potentiel écotoxique des estuaires du bassin.

⮚ La / les finalité(s) du ou des traitement(s) sont : contacter l’entreprise en charge des prélèvements.

⮚ Les données à caractère personnel traitées sont :

nom, prénom

e-mail

téléphone

adresse

autre : [Ajouter autant de case à cocher que de données collectées]

⮚ Les typologies de personnes concernées par la collecte de données à caractère personnel sont : employés de l’entreprise en charge des prélèvements.

**ARTICLE 3 - Durée du marché**

Le présent marché entre en vigueur à compter de la date de sa notification.

La présente annexe s’applique durant toute la durée de validité et d’exécution du marché, renouvellements et prolongations inclus.

# ARTICLE 4 - Obligations du sous-traitant vis-à-vis du/de la responsable de traitement

Le Sous-traitant s'engage à :

⮚ Traiter les données uniquement pour la ou les seule(s) finalité(s) décrite(s) dans la présente annexe.

⮚ Traiter les données conformément aux instructions documentées du Responsable de traitement, jointes le cas échéant à la présente annexe. 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 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 de traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs d'intérêt public.

⮚ Garantir la confidentialité des données à caractère personnel décrites dans la présente clause.

⮚ Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu de la présente clause :

* s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
* aient été informées ou aient reçu 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.
* aident, le cas échéant, le Responsable de traitement pour la réalisation d’analyses d’impact relatives à la protection des données ainsi que pour la réalisation de la consultation préalable de l’autorité de contrôle.
* mettent en œuvre les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté aux risques possibles et notamment :
* pseudonymisation et le chiffrement des données à caractère personnel ;
* mise en œuvre des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
* mise en œuvre 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;
* mise en place d’une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

⮚ Prendre en charge la réponse aux demandes des personnes identifiables exerçant leurs droits d’accès et de rectification des données à caractère personnel les concernant et informer le responsable de traitement des demandes et des réponses apportées par le Sous-Traitant

ou

⮚ Transmettre les demandes des personnes identifiables exerçant leurs droits d’accès et de rectification des données à caractère personnel les concernant dans un délai de 72h (jours ouvrés – à compter de la prise de connaissance au Responsable de traitement) par courriel à l’adresse du délégué à la protection des données à caractère personnel suivante : [dpd@aesn.fr](mailto:dpd@aesn.fr).

⮚ Le Sous-traitant, au stade de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec le Responsable de traitement avant la collecte de données.

**ARTICLE 5 - Obligations du Responsable de traitement vis-à-vis du Sous-traitant**

Le Responsable de traitement s’engage à :

⮚ Fournir au Sous-traitant les données visées à l’article 2 ci-dessus.

⮚ 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 européen sur la protection des données de la part du Sous-traitant,

⮚ Superviser le traitement, y compris réaliser les audits et les éventuelles inspections auprès du Sous-traitant.

**ARTICLE 6 - Sous-traitance ultérieure (au sens du Code de la Commande publique)**

Le Sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du Responsable de traitement. Il appartient au Sous-traitant initial (titulaire du marché) 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 traitement de l’exécution par l’autre Sous-traitant de ses obligations.

# ARTICLE 7 - Notification des violations de données à caractère personnel

⮚ Le Sous-traitant notifie par écrit le Responsable de traitement, de toute violation de données à caractère personnel dans un délai maximum de 3 jours ou dans les meilleurs délais, après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable du traitement, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente. 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 ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures que le Responsable de traitement doit 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.

**ARTICLE 8 - Sort des données**

⮚ Au terme de la prestation relative au traitement de ces données, le Sous-traitant s’engage à, (*cocher la case correspondante)* :

* [option 1]  - détruire toutes les données à caractère personnel. Une fois détruites, le sous-traitant justifie par écrit de la destruction.
* [option 2]  - renvoyer toutes les données à caractère personnel au Responsable de traitement. Le renvoi s’accompagne de la justification par écrit de la destruction de toutes les copies existantes dans les systèmes d’informations du sous-traitant.
* [option 3] - renvoyer les données à caractère personnel au Sous-traitant désigné par le Responsable de traitement (en cas de portabilité). 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 justifie par écrit de la destruction.

**ARTICLE 9 - Protection des données**

**Le Sous-traitant est soumis au RGPD** et a désigné un délégué à la protection des données (DPD), conformément à l’article 37 du RGPD, et de ce fait, doit communiquer les coordonnées du DPD au Responsable de traitement : ……………………………………………………………….

**Le Sous-traitant n’est pas soumis au RGPD** et, dans ce cas uniquement, communique les coordonnées de contact du représentant du titulaire, en précisant sa fonction : ………………………………………

**ARTICLE 10 - Registre des catégories d’activités de traitement**

⮚ Le Sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement effectuées pour le compte du/de la 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 effectues pour le compte du Responsable de 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 vises 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 ;
* la description générale des mesures de sécurité techniques et organisationnelles, mises en œuvre selon les besoins.

**ARTICLE 11 - Documentation**

Le Sous-traitant met à la disposition du Responsable de traitement, la documentation nécessaire pour démontrer le respect de toutes ses obligationset pour permettre la réalisation d'audits, y compris des inspections, par le/la Responsable de traitement ou un autre auditeur qu'il a mandaté. En cas de litige, les règles relatives au manquement à l’exécution sont celles mentionnées dans les documents du marché.

Fait en un exemplaire

|  |  |
| --- | --- |
| **Pour le Sous-traitant :**  Le | **Le Responsable de traitement**  Le  **La Directrice générale de l’Agence de l’eau Seine-Normandie** |