|  |
| --- |
| **Annexe à l’Acte d’Engagement**  **CONTRAT DE SOUS-TRAITANCE DE DONNEES** |

**PREAMBULE**

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 depuis le 25 mai 2018 (ci-après, le « **RGPD** »).

Dans le cadre des services mentionnés au Contrat, le Client ainsi que ses fournisseurs de données peuvent être amené(s) à communiquer au Prestataire des données à caractère personnel. Au sens de l’article 4 points (7) et (8) du RGPD, le Client est responsable du traitement et le Prestataire est sous-traitant des données à caractère personnel.

1. **OBJET**

La présente Annexe a pour objet de définir les conditions dans lesquelles le Prestataire s’engage à effectuer pour le compte du Client les opérations de traitement de données à caractère personnel définies ci-après, et assure leur protection et leur traitement conformément à la réglementation applicable mentionnée ci-dessus.

1. **DEFINITIONS**

« **Données Personnelles** » désignent 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 numéro d’identification ou à un ou plusieurs éléments qui lui sont propres.

« **Personne Concernée** » désigne une personne physique dont les Données Personnelles sont traitées.

« **Responsable du Traitement** » désigne la personne qui détermine les finalités et les moyens du Traitement des Données Personnelles.

« **Fournisseur de données** » désigne tout organisme possédant des données pouvant présenter un intérêt pour l’étude TRACY. Sans être exhaustif, il peut s’agir des sociétés impliquées dans le secteur nucléaire telles qu’Orano, le CEA, Framatome ou EDF, un centre de médecine du travail, etc.

« **Sous-traitant** » désigne la personne qui traite des Données Personnelles sous l’autorité, sur instructions et pour le compte du Responsable du Traitement.

« **Traitement** » désigne toute opération ou tout ensemble d’opérations portant sur des Données Personnelles par le Prestataire pour le compte du Client, quel que soit le procédé utilisé, et notamment la collecte, l’enregistrement, l’organisation, la structuration, 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 la limitation, l’effacement ou la destruction.

« **Violation de Données personnelles** » désigne une violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la corruption, le détournement de finalité, la compromission de la confidentialité ou la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données.

En cas de conflit ou d’ambiguïté entre les dispositions de la présente Annexe et celles du Contrat, les dispositions de la présente Annexe prévaudront.

1. **DESCRIPTION DU TRAITEMENT FAISANT L’OBJET DE LA SOUS-TRAITANCE**
   1. Le Prestataire est autorisé à traiter, pour le compte du Client, les Données Personnelles figurant dans les documents papiers et/ou électroniques mis à disposition pour le Client par les fournisseurs de données dans le cadre de l’étude épidémiologique TRACY. Le Prestataire ne peut traiter les Données Personnelles pour d’autres finalités que celles décrites dans le Contrat sans autorisation écrite et préalable du Client.
   2. Le Client détermine sous sa responsabilité les finalités des traitements confiés au Prestataire, lesquels sont les suivantes :

* Numérisation et saisie de documents relatifs à la santé, l’exposition ou l’historique de carrière des travailleurs de l’Etude TRACY
  1. Les Données Personnelles traitées sont :
* des données identifiantes des travailleurs (noms, prénoms, sexe, date et lieu de naissance, numéro de sécurité sociale)
* des données relatives à leurs expositions (radiologiques, chimiques, physique comme la chaleur et le bruit, travail posté …)
* des données relatives à leurs historiques de carrière (sociétés, types de contrat, affectations, qualifications, emplois occupés, motif de départ, lieu de départ …)
* des données relatives à leur santé provenant du dossier médical professionnel (taille, poids, Indice de Masse Corporelle, tensions, analyses de sang / urine / selles, pathologies : antécédents et incidentes, consommation de tabac / d’alcool, traitements, radiographies pulmonaires, éventuellement date et cause de décès …)

La durée des traitements mis en œuvre par le Prestataire pour le Client correspond à la durée du contrat.

1. **OBLIGATIONS DU PRESTATAIRE VIS-A-VIS DU CLIENT**
   1. Le Prestataire s'engage à :

* Ne traiter les Données Personnelles que pour les seules finalités qui font l’objet de la sous-traitance.
* Traiter les Données Personnelles conformément aux instructions documentées du Client, à moins que le Prestataire ne soit tenu d’y procéder en vertu du droit applicable au Contrat. Dans ce cas, le Prestataire informera le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs d’intérêt public. Si le Prestataire considère qu’une instruction constitue une violation du RGPD 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 le Client par écrit.
* Garantir la confidentialité des Données Personnelles traitées dans le cadre du Contrat et en particulier empêcher leur destruction, fuite, déformation, atteinte ou divulgation à des tiers non autorisés.
* Veiller à ce que les personnes autorisées à traiter les Données Personnelles dans le cadre des services :
  + 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.
* Prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des Données Personnelles dès la conception et par défaut.
* Proposer des prestations respectueuses des principes de proportionnalité, de minimisation et de limitation des Données Personnelles, afin que seules les données pertinentes telles que visées à l’Article 3.2 de la présente Annexe ne soient traitées.
  1. Le Prestataire est responsable de son personnel, de ses salariés et sous-traitants, et de leur respect des obligations lui incombant en vertu de la présente Annexe. A cet égard, le personnel du Prestataire ne pourra accéder aux Données Personnelles, les utiliser, les modifier, sauf lorsque cela est strictement nécessaire aux fins de la fourniture des services tels que mentionnés au Contrat, de la prévention ou du traitement des problèmes techniques ou pour en assurer la sécurisation.

Le Sous-traitant met en place des mesures organisationnelles et techniques pour s’assurer du respect par son personnel de ses obligations notamment en termes de contrôle des personnes habilitées à accéder aux données, de sécurisation des accès et de traçabilité. Il en tient la description détaillée à la disposition du Client.

* 1. Le Prestataire s’engage à ne transférer aucune Donnée Personnelle en dehors de ses locaux sécurisés. Il est interdit au Prestataire de photocopier et de numériser les questionnaires pour des finalités autres que celles qui font l’objet de la sous-traitance. Il est interdit au Prestataire de reporter les Données Personnelles sur un quelconque support autre que l’interface de saisie dédiée.
  2. Le Prestataire reconnaît qu’il doit être en mesure, dans un délai raisonnable et pendant toute l’exécution des services, de rendre compte et de faire la preuve de l’ensemble des procédures et des dispositifs de protection des Données Personnelles, de minimisation de leur utilisation, et de conformité aux exigences légales susmentionnées.
  3. Le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations en vertu de la présente Annexe et du RGPD.

1. **OBLIGATIONS DU CLIENT VIS-A-VIS DU PRESTATAIRE**
   1. Le Client s’engage à :

* Collecter sous sa responsabilité, de manière licite, loyale et transparente, les Données Personnelles fournies au Prestataire pour exécution des services. Il vérifiera notamment la base légale de cette collecte ainsi que le bon respect des dispositions relatives à l’information des Personnes Concernées ;
* Fournir au Prestataire les Données Personnelles nécessaires pour le Traitement, à l’exclusion de toute Donnée Personnelle non pertinente, disproportionnée ou non nécessaire, et à l’exclusion de toute Donnée « particulière » au sens du RGPD, sauf si les traitements et finalités le justifient, à charge pour le Client d’établir ces justifications et de prendre toutes mesures, notamment d’information préalable, de recueil de consentement et de sécurité, appropriées ;
* Documenter par écrit toute instruction concernant le Traitement des Données Personnelles par le Prestataire dans le respect des finalités convenues ;
* Veiller, au préalable et pendant toute la durée du Traitement, au respect par le Prestataire des obligations prévues par le RGPD ;
* Respecter les obligations qui lui incombent en sa qualité de responsable du traitement en vertu du RGPD.

1. **COOPERATION**
   1. En cas de demande d’une Personne concernée auprès du Client (notamment demande d’accès, de modification, d’effacement, d’opposition, de limitation ou de portabilité) nécessitant l’aide du Prestataire, ce dernier s’engage à apporter dans les meilleurs délais son concours au Client afin que ce dernier soit en mesure de répondre dans les délais légaux impartis à ladite Personne concernée.

Si une Personne Concernée envoie directement une demande au Prestataire, celui-ci doit en informer le Client dans les meilleurs délais par écrit à l’adresse suivante [dpo@asnr.fr](mailto:dpo@asnr.fr) et doit agir selon les instructions du Client.

* 1. Le Prestataire s’engage à collaborer loyalement et dans un délai raisonnable avec le Client dans le cadre de réalisation d’analyses d’impact relatives à la protection des Données Personnelles.
  2. Le Prestataire s’engage à coopérer loyalement et dans un délai raisonnable avec le Client dans le cadre de consultations préalables des autorités de contrôle.

1. **SOUS-TRAITANCE**
   1. Le Prestataire n’est pas autorisé par le Client à faire appel à des sous-traitants pour réaliser des activités de traitements spécifiques.
2. **NOTIFICATION DES VIOLATIONS DE DONNEES PERSONNELLES ET INCIDENT DE SECURITE**
   1. Le Prestataire s’engage à informer le Client, dans les meilleurs délais, de la survenance de tout incident, tant physique que technique, relatif à la sécurité ou à la confidentialité des Données Personnelles.
   2. Le Prestataire notifie par courrier électronique au Client la survenance de toute violation de Données Personnelles. La notification est adressée au Client à l’adresse suivante [dpo@asnr.fr](mailto:dpo@asnr.fr) dans les meilleurs délais et dans tous les cas dans les vingt-quatre (24) heures à compter de la survenance de la violation de Données Personnelles. La notification faite au Client contient au moins :

* la description de la nature de la violation de Données Personnelles 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 Personnelles concernés ;
* le nom et les coordonnées du Délégué à 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 Données Personnelles ;
* la description des mesures à mettre en œuvre pour remédier à la violation de Données Personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

1. **SECURITE DES DONNEES** 
   1. Le Prestataire s’engage à prendre toutes précautions utiles afin de préserver la confidentialité et la sécurité des Données Personnelles et notamment d’empêcher qu’elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. Plus généralement, le Prestataire s’engage à mettre en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les Données Personnelles contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération, la diffusion ou l’accès non autorisé aux Données Personnelles.
   2. Le Prestataire s’engage à prendre toutes mesures afin (i) de garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, (ii) de rétablir la disponibilité des Données Personnelles et l’accès à celles-ci dans les délais appropriés en cas d’incident physique ou technique et (iii) de tester, analyser et évaluer régulièrement l’efficacité de ces mesures.
   3. Le Prestataire tient à la disposition du Client les documents relatifs à la sécurité des Données Personnelles comprenant notamment la documentation technique nécessaire, les analyses de risques et la liste détaillée des mesures de sécurité mises en œuvre.
2. **DELEGUE A LA PROTECTION DES DONNEES**

Le Prestataire communique au Client le nom et les coordonnées de son DPO, s’il en a désigné un conformément à l’article 37 du RGPD.

1. **REGISTRE DES CATEGORIES D’ACTIVITE DES TRAITEMENTS**

Le Prestataire s’engage, dans la mesure où il remplirait les conditions d’établissement d’un registre conformément à l’article 30.5 du RGPD, à en tenir un par écrit de toutes les catégories d’activités de traitement effectuées pour le compte du Client comprenant l’ensemble des éléments mentionnés à l’article 30.2 du RGPD.

1. **AUDIT**

Le Client a la possibilité, à ses frais, d’auditer ou de faire auditer les dispositifs de protection internes des Données Personnelles mis en place par le Prestataire une fois par an, afin de vérifier la conformité du Prestataire à la présente Annexe et au RGPD. Le Prestataire s’engage à mettre à la disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations.

1. **SORT DES DONNEES PERSONNELLES**

Au terme du Contrat, le Prestataire s’engage à retourner l’ensemble des Données Personnelles traitées, comme précisé dans le cahier de clauses techniques particulières (CCTP).

**Signature du contrat par le titulaire individuel :**

|  |  |  |
| --- | --- | --- |
| **Nom, prénom et qualité**  **du signataire (\*)** | **Lieu et date de signature** | **Signature** |
|  | **A**  **le** |  |

**Signature du contrat par le pouvoir adjudicateur :**

**A : Montrouge, le**

|  |
| --- |
| **Pour l’ASNR,**  **Le Président**  **Monsieur Pierre-Marie ABADIE**  **Par délégation** |
| **Signature** |