**CONTRAT DE SOUS-TRAITANCE RGPD**

**Clauses contractuelles types en cas de recherche impliquant la personne humaine/ sur données mettant en œuvre ou impactant un (des) traitement(s) de données à caractère personnel**

ENTRE le CHU Saint-Etienne sis 25 boulevard Pasteur 42100 Saint-Etienne et représenté par M Olivier BOSSARD (Directeur Général) (ci-après dénommé le « ***RESPONSABLE DE TRAITEMENT***»)

d’une part,

ET […], situé à […] et représenté par […] (ci-après dénommé le « ***sous-traitant*** »)

d’autre part,

Il est convenu ce qui suit :

**I. Objet**

Les présentes clauses ont 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 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 »), et la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles (dite « Loi relative à la protection des données personnelles »).

**II. Description du traitement faisant l’objet de la sous-traitance**

Le SOUS-TRAITANT est autorisé à traiter pour le compte du RESPONSABLE DE TRAITEMENT les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [………..].

La nature des opérations réalisées sur les données est [……………].

La ou les finalité(s) du traitement sont [……………...].

Les données ou catégories de données à caractère personnel traitées sont [………………].

Les catégories de personnes concernées sont [………………].

Pour l’exécution du service objet du présent contrat, le RESPONSABLE DE TRAITEMENTmettent à la disposition du SOUS-TRAITANT les informations nécessaires suivantes […………..…].

**III. Durée du contrat**

Le présent contrat entre en vigueur à compter du 1er janvier 2025 pour une durée de 12 mois reconductible 3 fois 12 mois.

**IV. Obligations du SOUS-TRAITANT vis-à-vis du RESPONSABLE DE TRAITEMENT**

**IV.1. Traitement des données**

Le SOUS-TRAITANT s'engage à :

1. ne traiter les données **que pour la(les) seule(s) finalité(s)** qui fait (font) l’objet de la sous-traitance ;

2. traiter les données **conformément aux instructions documentées** du RESPONSABLE DE TRAITEMENTfigurant en annexe du présent contrat. 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 Etats 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’Etat membre auquel il est soumis, il doit informer le RESPONSABLE DE TRAITEMENTde cette obligation juridique avant le traitement, 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 contrat ;

4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :

* 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 ;
* prennent connaissance expressément de la politique générale de protection de l’information et de la charte d’utilisation des ressources informatiques, dans leurs versions en vigueur au sein du RESPONSABLE DE TRAITEMENT pendant la durée du présent contrat ;
* Soient soumises à des obligations de discrétion professionnelle, ou le cas échéant au secret professionnel, les personnels du SOUS-TRAITANT sont régulièrement sensibilisés sur leurs rôles et responsabilités en matière de confidentialité et de sécurité des données ;
* agissent sur instruction du responsable de la sécurité des systèmes d’information, du responsable de la protection de l’information, du délégué à la protection des données à caractère personnel ou de leurs représentants ;

5. 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, au sens de l’article 25 du règlement européen sur la protection des données ;**

**IV.2. Sous-traitance**

*Choisir l’une des deux options*

***Option A*** *(autorisation générale)*

Le SOUS-TRAITANT peut faire appel à un autre sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le RESPONSABLE DE TRAITEMENTde tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du SOUS-TRAITANT et les dates du contrat de sous-traitance. Le RESPONSABLE DE TRAITEMENTdispose d’un délai minium de […] à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le RESPONSABLE DE TRAITEMENTn'a pas émis d'objection pendant le délai convenu.

***Option B*** *(autorisation spécifique)*

Le sous-traitant est autorisé à faire appel à l’entité [….…] pour mener les activités de traitement suivantes : [……..]

En cas de recrutement d’autres sous-traitants, le SOUS-TRAITANT doit recueillir l’autorisation écrite, préalable et spécifique du RESPONSABLE DE TRAITEMENT.

***Quelle que soit l’option*** *(autorisation générale ou spécifique)*

Le sous-traitant 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 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 du SOUS-TRAITANT ne remplit pas ses obligations en matière de protection des données, le SOUS-TRAITANT demeure pleinement responsable devant le RESPONSABLE DE TRAITEMENTde l’exécution de ses obligations par un sous-traitant du SOUS-TRAITANT.

**IV.3. Droit d’information des personnes concernées**

*Choisir l’une des deux options*

***Option A***

Il appartient au RESPONSABLE DE TRAITEMENTde fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

***Option B***

Le SOUS-TRAITANT, au moment 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 TRAITEMENTavant la collecte de données.

**IV.4. Exercice des droits des personnes**

Dans la mesure du possible, le SOUS-TRAITANT doit aider le RESPONSABLE DE TRAITEMENTà 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).

***Choisir l’une des deux options***

***Option A***

Lorsque les personnes concernées exercent auprès du SOUS-TRAITANT des demandes d’exercice de leurs droits, le SOUS-TRAITANT doit adresser ces demandes dès réception par courrier électronique à […] (*indiquer un contact au sein du RESPONSABLE DE TRAITEMENT*).

***Option B***

Le SOUS-TRAITANT doit répondre, au nom et pour le compte du RESPONSABLE DE TRAITEMENTet dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d’exercice de leurs droits, s’agissant des données faisant l’objet de la sous-traitance prévue par le présent contrat.

**IV.5. Notification des violations de données à caractère personnel**

Le SOUS-TRAITANT notifie au RESPONSABLE DE TRAITEMENTtoute violation de données à caractère personnel dans un délai maximum de […] heures après en avoir pris connaissance et par email à l’adresse [………..…]. Cette notification est accompagnée de toute documentation utile afin de permettre au RESPONSABLE DE TRAITEMENT, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

***Option possible***

Après accord du RESPONSABLE DE TRAITEMENT, le SOUS-TRAITANT notifie à l’autorité de contrôle compétente (la CNIL), au nom et pour le compte du RESPONSABLE DE TRAITEMENT, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques.

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 données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement 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.

Après accord du RESPONSABLE DE TRAITEMENT, le SOUS-TRAITANT communique, au nom et pour le compte du RESPONSABLE DE TRAITEMENT, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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 données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement 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.

**IV.6. Aide du SOUS-TRAITANT dans le cadre du respect par le RESPONSABLE DE TRAITEMENT de ses obligations**

Le SOUS-TRAITANT aide le RESPONSABLE DE TRAITEMENTpour la réalisation d’analyses d’impact relative à la protection des données.

Le SOUS-TRAITANT aide le RESPONSABLE DE TRAITEMENTpour la réalisation de la consultation préalable de l’autorité de contrôle.

**IV.7. Mesures de sécurité**

Le SOUS-TRAITANT s’engage à mettre en œuvre les mesures de sécurité suivantes :

[*Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres*

* *la pseudonymisation 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]*

Le SOUS-TRAITANT s’engage à mettre en œuvre les mesures de sécurité prévues par [*code de conduite, certification*].

[*Dans la mesure où l’article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au SOUS-TRAITANT, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre*]

**IV.8. Sort des données**

Au terme du traitement de ces données, le SOUS-TRAITANT s’engage à :

*Au choix des parties :*

* détruire toutes les données à caractère personnel ou
* à renvoyer toutes les données à caractère personnel au RESPONSABLE DE TRAITEMENT ou
* à renvoyer les données à caractère personnel au SOUS-TRAITANT désigné par le RESPONSABLE DE TRAITEMENT

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 doit justifier par écrit de la destruction.

**IV.9. Délégué à la protection des données**

Le SOUS-TRAITANT communique au RESPONSABLE DE TRAITEMENT **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

**IV.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 RESPONSABLE DE TRAITEMENTcomprenant :

* 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 effectués 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 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 et le chiffrement des données à caractère personnel;
  + des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  + 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;
  + une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

**IV.11. Documentation**

Le SOUS-TRAITANT met à la disposition du RESPONSABLE DE TRAITEMENTla **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le RESPONSABLE DE TRAITEMENTou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

**V. Obligations du RESPONSABLE DE TRAITEMENT vis-à-vis du SOUS-TRAITANT**

Le RESPONSABLE DE TRAITEMENTs’engage à :

1. fournir au SOUS-TRAITANT les données visées au II des présentes clauses ;

2. documenter par écrit toute instruction concernant le traitement des données par le SOUS-TRAITANT ;

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 SOUS-TRAITANT ;

4. superviser le traitement, y compris réaliser les audits et les inspections auprès du SOUS-TRAITANT.

Fait à \_\_\_\_\_\_\_\_\_\_\_\_, en deux (2) exemplaires originaux,

|  |  |
| --- | --- |
| Pour le RESPONSABLE DE TRAITEMENT  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date : | Pour le SOUS-TRAITANT  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date : |

**ANNEXE : Instructions du RESPONSABLE DE TRAITEMENT relatives au traitement des données**

### ***Obligation de conseil du SOUS-TRAITANT***

*Le SOUS-TRAITANT s’engage à conseiller le RESPONSABLE DE TRAITEMENT sur l’application du Règlement Général de Protection des Données dès lors qu’il considère qu’une non-conformité peut avoir un impact que le respect de clauses du présent contrat.*

### ***Communication de données à des tiers autorisés***

*Le SOUS-TRAITANT s’engage à informer sans délai le RESPONSABLE DE TRAITEMENT en cas de requête provenant d’une autorité administrative ou judiciaire demandant à avoir communication de données à caractère personnel entrant dans le périmètre du présent contrat.*

*Dans le cas où la requête est reçue par le RESPONSABLE DE TRAITEMENT, le SOUS-TRAITANT s’engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés sur le périmètre des opérations de traitement sous-traitées.*

### ***Engagement relatif aux contrôles et aux audits***

*Le SOUS-TRAITANT s’engage à répondre aux demandes d’audit du RESPONSABLE DE TRAITEMENT, effectuées par lui-même ou par un tiers de confiance qu’il aura sélectionné et s’engage à mettre en œuvre les moyens permettant à l’auditeur de réaliser sa mission dans les meilleures conditions.*

*Le RESPONSABLE DE TRAITEMENT s’engage à fournir au SOUS-TRAITANT une copie du rapport d’audit afin qu’il puisse prendre en compte rapidement les non-conformités constatées et les mesures correctives proposées.*

*Le SOUS-TRAITANT s’engage à mettre en œuvre les mesures correctives nécessaires au traitement des non-conformités identifiées dans un délai et selon les conditions définies d’un commun accord.*

*Dans le cas ou des mesures correctives ne seraient pas applicables, le SOUS-TRAITANT s’engage à justifier l’impossibilité de mettre en œuvre les mesures et s’engage à proposer des mesures palliatives pour réduire les risques encourus.*

### ***Engagement relatif au traitement des réclamations***

*Le SOUS-TRAITANT s’engage à informer sans délai le RESPONSABLE DE TRAITEMENT pour toute demande qu’il reçoit des personnes concernées par les opérations de traitement sous-traitées.*

*Le SOUS-TRAITANT s’engage à aider le RESPONSABLE DE TRAITEMENT lors du traitement d’une réclamation d’une personne concernée et s’engage à mettre en œuvre les moyens permettant de traiter les demandes dans le délai de 1 mois imposé par le Règlement Général de Protection des Données.*

*Dans le cas où le SOUS-TRAITANT ne serait pas en capacité de fournir les éléments permettant au RESPONSABLE DE TRAITEMENT de respecter le délai de 1 mois, il s’engage à fournir les justificatifs permettant au RESPONSABLE DE TRAITEMENT d’informer le demandeur sur les difficultés rencontrées et il s’engage à mettre en œuvre les moyens pour traiter les demandes dans un délai maximum de 50 jours après la première sollicitation.*

### ***Engagement du SOUS-TRAITANT en tant que responsable de traitement***

*Le SOUS-TRAITANT s’engage à respecter les obligations qui lui incombent en tant que responsable de traitement et à fournir au RESPONSABLE DE TRAITEMENT des éléments de traçabilité permettant de le démontrer.*

*Le Délégué à la Protection des Données du SOUS-TRAITANT se tiendra à la disponibilité du RESPONSABLE DE TRAITEMENT pour apporter les éléments justificatifs démontrant l’application du Règlement Général de Protection des Données. Son interlocuteur privilégié sera le Délégué à la Protection des Données du RESPONSABLE DE TRAITEMENT (XXXX).*

### ***Devoir de coopération avec l’autorité de Contrôle (CNIL)***

*Le SOUS-TRAITANT s’engagent à coopérer avec l’autorité de contrôle compétente en matière de protection des données (CNIL), notamment en cas de demande d’information qui pourrait être adressée par cette dernière, ou en cas de contrôle sur site ou à distance des opérations de traitement sous-traitées.*

*Le SOUS-TRAITANT s’engage à informer le RESPONSABLE DE TRAITEMENT en cas de contrôle sur site ou à distance des opérations de traitement sous-traitées et à remettre le cas échéant une copie du rapport de l’autorité de contrôle.*

### ***Engagement en matière de sécurité des données***

*Le SOUS-TRAITANT s’engage à prendre toutes précautions utiles afin de préserver la sécurité des données et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées (conformément à l’article 32 du Règlement Général de Protection des Données).*

*Le SOUS-TRAITANT s’engage notamment à mettre en œuvre :*

* *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
* *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;*
* *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.*

*Le SOUS-TRAITANT s’engage à respecter les bonnes pratiques en matière de sécurité émises par les autorités compétentes (ANSSI notamment) et à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. La cartographie des risques réalisée par le SOUS-TRAITANT pourra être présentée sur demande au RESPONSABLE DE TRAITEMENT.*

*Le RESPONSABLE DE TRAITEMENT pourra à tout moment solliciter le Responsable de la Sécurité des Systèmes d’Information (RSSI) du SOUS-TRAITANT pour s’assurer que la politique spécifique de sécurité mise en œuvre sur le périmètre du présent contrat est appliquée et respecte les bonnes pratiques reconnues dans le domaine ainsi que les exigences du Règlement Général de Protection des Données.*