

HEBERGEMENT ET TIERCE MAINTENANCE APPLICATIVE DE L'OUTIL DE GESTION DES ABONNEMENTS AU MAGAZINE DE L'INSERM

Contrat d'engagement RGPD

Traitement de données à caractère personnel

1.1. Objet

La présente clause a pour objet de définir les conditions dans lesquelles le titulaire, en tant que sous-traitant de l'Inserm (ci-après désigné le « Sous-traitant »), s'engage à effectuer pour le compte de l'Inserm, en tant que responsable de traitement (ci-après désigné le « Responsable de traitement »), les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, le Titulaire et l'Inserm (ci-après « les Parties ») s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel en particulier la loi du 6 janvier 1978 n°78-17 relative à l'informatique, aux fichiers et aux libertés modifiée et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après ensemble ou séparément « la Réglementation relative à la protection des données ») ainsi que toute évolution législative ou réglementaire qui pourrait survenir pendant toute la durée du marché et qui serait applicable aux données à caractère personnel.

À ce titre, le titulaire s'engage à traiter les données à caractère personnel confiées par l'Inserm dans le respect de ses instructions écrites et des dispositions prévues au présent article, que le titulaire déclare expressément être en mesure de respecter.

Aux fins de la présente clause, les termes de « données à caractère personnel », « traitement », « sous-traitant », « responsable de traitement », « destinataire » et « violation de données à caractère personnel » doivent être entendus au sens du Règlement européen sur la protection des données.

1.2. Description des traitements faisant l'objet de la sous-traitance

- Les traitements de données à caractère personnel ont les finalités suivantes :
 - o La gestion des abonnements au magazine de l'Inserm,
 - o La mise à disposition d'un serveur sécurisé pour la gestion des abonnés et l'export routage imprimeur.
- Les principales catégories de données à caractère personnel collectées sont :
 - o Les adresses postales et/ou e-mail des personnes et leur type d'abonnement.
- Les personnes concernées sont :
 - o Les agents Inserm,
 - o Le grand public,
 - o Les institutionnels.
- Les principaux destinataires de ces données à caractère personnel sont :
 - o Les agents du département de la communication de l'Inserm,
 - o L'imprimeur chargé du routage postal.

- Pour l'exécution du service objet du présent contrat, le Responsable de traitement met à la disposition du Sous-traitant les informations nécessaires détaillées dans le présent marché.
- Le Délégué à la protection des données du Responsable de traitement peut être contacté par courrier électronique à l'adresse dpo@inserm.fr ou par courrier postal à l'attention du Délégué à la protection des données, 101 rue de Tolbiac 75013 Paris.

1.3. Obligations des Parties

i. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à :

1. traiter les données uniquement pour la ou 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 traitement figurant au 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 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 du traitement de 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 ;
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.

6. Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant (ci-après « le Sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de traitement de 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 traitement dispose d'un délai minimum de 30 (trente) jours 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 traitement n'a pas émis d'objection pendant le délai convenu.

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 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 règlement européen sur la protection des données. 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 de traitement de l'exécution par l'autre sous-traitant de ses obligations. À ce titre, le Sous-traitant mettra à disposition du Responsable de traitement la liste de l'ensemble de ses Sous-traitants du Service.

7. Droit d'information des personnes concernées

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 traitement avant la collecte de données.

8. Exercice des droits des personnes

Dans la mesure du possible, le Sous-traitant doit aider le Responsable de traitement 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).

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 dpo@inserm.fr ou par courrier postal à l'attention du Délégué à la protection des données, 101 rue de Tolbiac 75013 Paris.

9. Notification des violations de données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 (quarante-huit) heures après en avoir pris connaissance et par courrier électronique à l'adresse dpo@inserm.fr, puis confirmée par lettre recommandée avec accusé de réception à l'attention du Délégué à la Protection des Données, 101 rue de Tolbiac 75013 Paris. 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.

10. Aide du Sous-traitant dans le cadre du respect par le Responsable de traitement de ses obligations

Le Sous-traitant aide le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le Sous-traitant aide le Responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre toutes les mesures de sécurité nécessaires pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement. Il respecte les exigences du Responsable de traitement ainsi que la législation et la réglementation applicables.

Par ailleurs, le Sous-traitant s'interdit de :

- Divulguer, sous quelque forme que ce soit, tout ou partie des données à caractère personnel ;
- De prendre copie ou stocker, quelles qu'en soient la forme ou la finalité, tout ou partie des informations ou données à caractère personnel contenues sur les supports ou documents qui lui ont été confiés ou recueillies par lui au cours de

l'exécution de ses prestations prévues par le présent contrat si ces opérations ne sont pas réalisées dans le cadre des prestations du contrat.

Le Sous-traitant s'engage à 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.

Il met en œuvre toute mesure technique et organisationnelle appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

Le Sous-traitant met à disposition du Responsable de traitement la politique de sécurité des systèmes d'information qu'il a mis en place et l'informe des évolutions de cette politique. Il tient à disposition du Responsable de traitement les documents relatifs à la sécurité des données à caractère personnel comprenant notamment la documentation technique nécessaire, les analyses de risques produites et la liste détaillée des mesures de sécurité mises œuvres.

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le Sous-traitant s'engage, dans un délai de 12 mois après la phase de réversibilité, à :

- Détruire toutes les données à caractère personnel ou
- Renvoyer toutes les données à caractère personnel au 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.

13. 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.

14. 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 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 effectués pour le compte du Responsable du 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.

15. Documentation

Le Sous-traitant met à la disposition du Responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le Sous-traitant s'engage à coopérer avec la CNIL, notamment en cas de demande d'informations qui pourrait lui être adressée ou en cas de contrôle. À ce titre, le Sous-traitant convient que la CNIL a le droit d'effectuer des vérifications dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez le Responsable de traitement conformément à la législation et à la réglementation en vigueur et à venir relatives aux données à caractère personnel.

ii. 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 au paragraphe 1.2 *Description des traitements faisant l'objet de la sous-traitance*;
- 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 inspections auprès du Sous-traitant.

Fait en un seul original

À _____, le _____
Pour le Titulaire

À Paris, le _____
Pour l'Inserm